Symantec™ Protection Engine for Network Attached Storage 8.1 Software Developer's Guide

Symantec™ Protection Engine for Network Attached Storage 8.1 Software Developer's Guide

Legal Notice

This Symantec product may contain third party software for which Symantec is required to provide attribution to the third party (“Third Party Programs”). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. Please see the Third Party Legal Notice Appendix to this Documentation or TPIP ReadMe File accompanying this Symantec product for more information on the Third Party Programs.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec Support

All support services will be delivered in accordance with your support agreement and the then-current Enterprise Technical Support policy.

Knowledge Base Articles and Symantec Connect

Before you contact Technical Support, you can find free content in our online Knowledge Base, which includes troubleshooting articles, how-to articles, alerts, and product manuals. In the search box of the following URL, type the name of your product:

https://support.symantec.com

Access our blogs and online forums to engage with other customers, partners, and Symantec employees on a wide range of topics at the following URL:

https://www.symantec.com/connect

Technical Support and Enterprise Customer Support

Symantec Support maintains support centers globally 24 hours a day, 7 days a week. Technical Support's primary role is to respond to specific queries about product features and functionality. Enterprise Customer Support assists with non-technical questions, such as license activation, software version upgrades, product access, and renewals.

For Symantec Support terms, conditions, policies, and other support information, see:

https://entced.symantec.com/default/ent/supportref

To contact Symantec Support, see:

https://support.symantec.com/en_US/contact-support.html

Contents

Chapter 1

Getting started

This chapter includes the following topics:

About Symantec Protection Engine for Network Attached Storage

Symantec™ Protection Engine for Network Attached Storage is hereafter referred to as Symantec™ Protection Engine.

Symantec™ Protection Engine is a carrier-class, network-accessible, and content-scanning engine. Symantec Protection Engine provides content scanning capabilities to any application on an IP network, regardless of platform.

Symantec Protection Engine features all of the key content-scanning technologies that are available in the complete line of Symantec products. Symantec Protection Engine is one of the most effective solutions available for protecting your network against a variety of undesirable content.

For more information, see the *Symantec Protection Engine Implementation Guide*.

About the software developer’s guide

Software developers can use the information that is provided in the *Symantec Protection Engine Software Developer’s Guide* to create client applications that let third-party applications integrate with Symantec Protection Engine for a variety of content scanning services. You can configure client applications to communicate with Symantec Protection Engine using one of several supported protocols. However, the only protocol that is supported in the software developer’s guide is the Internet Content Adaptation Protocol (ICAP) version 1.0, as presented in RFC 3507 (April 2003).

What's new in Symantec Protection Engine 8.1

Table 1-1 describes the new features in Symantec Protection Engine.

Table 1-1 New features

Feature	Description
Support for non-archive files larger than 2 GB	Symantec Protection Engine 8.1 supports the scanning of the non-archive files that are larger than 2 GB. The support is limited to 2 GB in previous releases.
Latest Symantec technologies	Symantec Protection Engine 8.1 is integrated with latest internal Symantec scanning technologies. Improved efficacy with the help of AML, x86 PE Emulator, nonPE/Scripts, etc.
Enhanced LiveUpdate	Internal critical fixes are now delivered through LiveUpdate.
Improved in-memory file system	Symantec Protection Engine uses the system memory to stream and scan the files. Now, the memory size is no more limited to 4 GB.

About integrating with Symantec Protection Engine

Symantec Protection Engine can be easily implemented in an existing infrastructure. Symantec Protection Engine runs on 64-bit platforms for Red Hat Linux and Windows Server. You can run Symantec Protection Engine on the same computer or a different computer than the client application

For more information about Symantec Protection Engine system requirements, see the *Symantec Protection Engine Implementation Guide*.

Software developers can create client applications (connectors) that let third-party applications integrate with Symantec Protection Engine for content scanning services using ICAP as the communication protocol.

You can create a custom integration using any of the following methods:

Construct an ICAP client connector using application program interface (API) C library.

If you plan to integrate antivirus scanning only, you can use the antivirus C API. URL filtering is not available using the antivirus API.

The antivirus API includes static and dynamic libraries for each supported platform. The API library consists of functions that provide scanning and repair services to client applications. The C API supports the FILEMOD and RESPMOD scanning modes, and it contains the built-in ability to stream files.

For more information, see Symantec_Protection_Engine_SDK\C\Docs\ in the Symantec Protection Engine documentation zip file.

Construct an ICAP client connector using Java API library.

If your environment has Java, you can use the Java API plug-in (SymJavaAPI.jar) to integrate with Symantec Protection Engine. The Java API provides client antivirus scanning and repair services using the ICAP protocol. The Java API supports the FILEMOD and RESPMOD scanning modes, and it contains the built-in ability to stream files.

For more information, see Symantec_Protection_Engine_SDK\Java\Docs\SymJavaAPIDocs.jar in the Symantec Protection Engine documentation zip file.

Construct an ICAP client connector using .NET API library.

If your environment has .NET Framework, you can use the .NET API plug-in (symcsmsnetapi.dll) to integrate with Symantec Protection Engine. The .NET API provides client antivirus scanning and repair services using the ICAP protocol. The .NET API supports the FILEMOD and RESPMOD scanning modes, and it contains the built-in ability to stream files.

For more information, see Symantec_Protection_Engine_SDK\CSharp\Docs\SymCSharpAPIDocs.chm in the Symantec Protection Engine documentation zip file.

Construct your own ICAP 1.0 client for the Symantec Protection Engine.

If you construct your own ICAP client, you can specify whether to perform antivirus scanning and URL filtering for outgoing and incoming requests.

For more information, see *Symantec™ Protection Engine Software Developer's Guide*.

About ICAP

ICAP is a lightweight protocol that was originally created to execute a remote procedure call on HTTP messages. ICAP is part of an evolving architecture that lets corporations, data communication companies, and Internet service providers (ISPs) dynamically scan, change, and augment data as it flows through ICAP servers. The protocol lets ICAP clients pass data to ICAP servers for adaptation (some type of transformation or other processing, such as virus or URL filtering). The server executes its transformation service on the data and responds to the client, possibly with modified content.

In a typical integration for processing HTTP traffic, a caching proxy server retrieves the requested information from the Web. At the same time, it caches the information (stores a copy on disk) and, where possible, serves multiple requests for the same Web content from the cache. A caching proxy server can use ICAP to communicate with Symantec Protection Engine and request that content that is retrieved from the Web be scanned and repaired, if necessary.

About the C API

You can use the client-side API C library to configure an application to pass files to Symantec Protection Engine for scanning. The API includes static and dynamic libraries for each supported platform. The API library consists of functions that provide scanning and repair services to client applications.

Table 1-2 lists the available platforms for Symantec Protection Engine API C library

Table 1-2 Platforms for Symantec Protection Engine API C library

Operating system	Architecture	Compiler
Red Hat Enterprise Linux 5.5	x64	using gcc 4.1.2
Red Hat Enterprise Linux 5.5	x86	using gcc 4.1.2
Solaris 10 (SPARC)	64bit	using gcc 3.4.3
Windows Server 2008 R2	x64	using Microsoft Visual Studio 2008, 2010, or 2013
Windows Server 2008	x86	using Microsoft Visual Studio 2008

A C header file is included at the following location:

```
<Product .zip file>/Symantec_protection_engine_SDK/C/Include/
```

About other protocols

Symantec Protection Engine supports Remote Procedure Call (RPC) 1.0 and 1.1 for Network Appliance (NetApp) Filer. This protocol is a proprietary implementation and is not documented by Symantec.

How to maximize performance

In a typical configuration, files are passed to Symantec Protection Engine through a socket over the network because Symantec Protection Engine is running on a separate computer. Depending on the network setup, client applications (applications that are configured to pass files to Symantec Protection Engine for scanning) can pass a full path rather than the actual file to Symantec Protection Engine for improved performance. For example, files to be scanned might be located on a drive that can be mounted over the network, such as a shared drive in Windows or a network file system (NFS) drive. If the client application and Symantec Protection Engine have access to a shared directory, the client application can place the file in the shared directory and pass the full path to Symantec Protection Engine.

For cases in which the client application is running on the same computer as Symantec Protection Engine, the client application can pass the file name to Symantec Protection Engine, and Symantec Protection Engine can open the file and scan it in place on the computer.

See “Local file scanning (FILEMOD)” on page 73.

About Symantec Protection Engine API load balancing

The Symantec Protection Engine API provides scheduling across any number of computers that are running Symantec Protection Engine. Client applications that pass files to Symantec Protection Engine benefit from load-balanced virus scanning without any additional effort. When multiple Protection Engines are used, the API determines the appropriate Protection Engine to receive the next file to be scanned. The determination is based on the scheduling algorithm.

Another Protection Engine is called when any of the following events occur:

- A Protection Engine is unreachable
- A Protection Engine stops responding during a scan
- If you use ICAP and the queued requests threshold is reached
  When the threshold is reached, Symantec Protection Engine rejects the scan request.

The faulty Protection Engine is taken out of rotation for a period of time (30 seconds is the default). If all of Symantec Protection Engines are out of rotation, the faulty Protection Engines are called again. The API does not stop trying to contact Symantec Protection Engines unless five engines do not respond. Or it appears that a file that is being scanned might have caused more than one engine to stop responding.

About licensing

Key features for Symantec Protection Engine are activated by license.

The content scanning features, including antivirus and URL filtering, are activated by product licenses. Subscription licenses let you obtain updates to virus definitions and URL filtering content updates. When a license expires, a new license must be installed.

When no product license is installed, Symantec Protection Engine is not operational. After you install a product license, you can access the relevant portions of the administrative interface, and Symantec Protection Engine is operational. For example, if you activate a product license for antivirus scanning only (with no URL filtering), you are not able to access those portions of the administrative interface that relate to URL filtering.

When no subscription license is installed or a subscription license expires, Symantec Protection Engine is operational, but updates are not permitted. New virus definitions updates are not downloaded to keep protection current, and URL-filtering updates to the URL lists are not permitted.

For more information about licensing, see the Activating licenses section*Symantec Protection Engine Implementation Guide*.

Where to start

Configuring client applications to use ICAP 1.0 to pass files to Symantec Protection Engine for scanning involves the following process:

- Become familiar with the design and features of the software.
  See also the *Symantec Protection Engine Implementation Guide*.
- Decide how to deploy Symantec Protection Engine to meet your specific requirements.
  See "Considerations for custom integration" on page 13.
- Install and configure Symantec Protection Engine to use ICAP as the communication protocol.
  For more information, see the *Symantec Protection Engine Implementation Guide*.
  See "About configuring Symantec Protection Engine" on page 14.
- Configure the client applications that will send files to Symantec Protection Engine for scanning.

Chapter 2

Configuring Symantec Protection Engine for custom integrations

This chapter includes the following topics:

Considerations for custom integration

Symantec Protection Engine is designed to be integrated into any environment to provide content scanning for any application. Client applications are configured to pass files to Symantec Protection Engine. Symantec Protection Engines performs the required functions and returns the request with the necessary changes. Symantec Protection Engine supports custom integrations in which the software developer creates a client application (connector) to provide content scanning services for a third-party application. The client application communicates with Symantec Protection Engine using ICAP 1.0.

You must configure Symantec Protection Engine to support the custom integration as follows:

- Selecting ICAP as the communication protocol
- Configuring ICAP-specific options
- Configuring the scanning parameters

You must decide how to configure the client application and Symantec Protection Engine to ensure that scanning is handled appropriately. This decision can depend on the capabilities of the third-party application.

For example, for antivirus scanning, the client application can decide which file types to scan and pass only the appropriate files to Symantec Protection Engine. In other cases, you can configure the client application to pass all files to Symantec Protection Engine. Then configure Symantec Protection Engine to scan those file types that are likely to contain viruses.

You must configure the client application to communicate with Symantec Protection Engine and to handle the results that are returned from Symantec Protection Engine.

How the application is configured to handle the results that are returned from Symantec Protection Engine can also depend on the capabilities of the third-party application, which includes, but is not limited to, the following:

- Blocking access to infected files or files that violate other configured policies
- Quarantining unrepairable files

For example, for content scanning, Symantec Protection Engine returns only the lookup results when you use audit mode. The client application applies the blocking policy based on the results. You can obtain information about configuring the client application to work with Symantec Protection Engine in audit mode by contacting Symantec Service and Support.

About configuring Symantec Protection Engine

Table 2-1 describes the minimum settings that you must configure for Symantec Protection Engine to perform scanning services.

Table 2-1 Symantec Protection Engine configuration options

Setting	Description
Select the ICAP protocol and configure protocol options	You must configure Symantec Protection Engine to use ICAP to communicate with clients that are running the proprietary version 1.0 of ICAP (RFC 3507, April 2003). Any appropriate client can use ICAP to communicate with Symantec Protection Engine to request scanning and repairing of files. You can configure multiple client applications that use different versions of ICAP to pass files to a single protection engine. If you select ICAP as the protocol to be used by Symantec Protection Engine, you must configure several ICAP-specific options. You must also configure the ICAP client to work with Symantec Protection Engine.
Configure antivirus settings	You can configure certain aspects of antivirus scanning, including the following options: ■ Adjusting Bloodhound sensitivity ■ Specifying file types to scan ■ Establishing a mail filter policy

Table 2-1 Symantec Protection Engine configuration options *(continued)*

Setting	Description
Specify processing limits	You can impose restrictions on the amount of resources that are used to handle individual files. These processing limits let you manage resources and protect your network against denial-of-service attacks.
Configure URL filtering settings	You can configure URL filtering settings, which includes the following options: ■ Specifying URL categories to deny ■ Specifying URLs to allow ■ Auditing URL sites rather than block access

For more information about how to configure these options, see the *Symantec Protection Engine Implementation Guide*.

Changing the ICAP response

In its default configuration, when ICAP is the communication protocol, Symantec Protection Engine sends a 201 Created response in the following scenarios:

- A virus was detected, but the file could not be repaired.
- A virus was detected and Symantec Protection Engine is configured for scan-only mode.

If a virus is detected and the file cannot be repaired or Symantec Protection Engine is configured for scan-only mode, Symantec Protection Engine includes a replacement file in the body of the response message. The message informs users that access to a file is being denied because it contains a virus or content violation.

Symantec Protection Engine default behavior deviates from the ICAP 1.0 standard, which does not support automatically sending a replacement file. In the ICAP 1.0 standard, this type of context-sensitive behavior is performed by the client rather than by Symantec Protection Engine.

If your client application closely follows the ICAP 1.0 standard, you might need to change Symantec Protection Engine default ICAP response setting to receive an ICAP 403 response instead of a replacement file. Symantec Protection Engine sends a 403 response if the file is denied based on Symantec Protection Engine policy setting. If the file is acceptable, Symantec Protection Engine returns a 200 OK response. You should change the default ICAP response setting only if you are sure that the client application supports this behavior.

To make this change, you must edit the configuration.xml file using the XML modifier tool. The XML modifier tool is provided on the Symantec Protection Engine product CD. This tool is automatically installed when you install the product.

For more information, see the *Symantec Protection Engine Implementation Guide*.

To change the ICAP response

1 In the XML modifier tool, at the command line, type the following command:

```
java -jar  xmlmodifier.jar
```

2 Type the following XPath:

```
/configuration/protocol/ICAP/ICAPResponse/@value
```

where @value is any of the following:

0	Send an ICAP 403 response
1	Send a replacement file. This is the default setting.

3 Stop and restart Symantec Protection Engine.

Chapter 3

Constructing clients using ICAP 1.0

This chapter includes the following topics:

How ICAP works

The Internet Content Adaptation Protocol (ICAP) is a request/response-based protocol that lets ICAP clients pass messages to ICAP servers for processing or adaptation. The client initiates the session by sending request messages over a TCP/IP connection to a passively waiting ICAP server on a designated port. (Port 1344 is the default ICAP port.)

The server then does the following:

- Runs the service that was requested, such as antivirus scanning
- Performs any transformations that are necessary, such as repairing an infected file
- Sends a response back to the client with any modified data

A single transport can be used for multiple request/response pairs. Requests are matched with responses by allowing only one outstanding request on a connection at a time. Multiple connections can be used.

About ICAP messages

ICAP clients and servers communicate through messages, which are similar in format to HTTP. ICAP messages consist of client requests and server responses. All ICAP messages consist of a start line, which includes a client request or server response (depending on the type of message), header fields, and the message body. A blank line precedes the message body to distinguish the headers from the message body.

Multiple HTTP message sections can be encapsulated in a single ICAP message for vectoring of requests, responses, and request/response pairs on an ICAP server.

Encapsulated messages must include an encapsulated header, which offsets the start of each encapsulated section from the start of the message body.

See "About encapsulated messages" on page 30.

Although request and response messages have unique headers, some headers are common to both requests and responses.

Table 3-1 lists the request/response headers that Symantec Protection Engine uses.

Table 3-1 Request/response headers

Header	Description
Connection	Specifies options that the message sender wants to use only for that connection and not for proxies over other connections. For example: Connection: close
Date	Provides the date and time that the message was created using standard HTTP date and time format. For example: Date: Tue, 5 July 2005 14:29:31 GMT

About ICAP requests

All ICAP client requests must start with a request line that includes the following components:

Method	ICAP command or operation to perform (for example, REQMOD)

Uniform Resource Identifier (URI)	Complete host name of the ICAP server and the path of the resource that is being requested
ICAP version	Version string for the current version of ICAP using the format ICAP/version number (for example ICAP/1.0)

The URI consists of the following components:

```
ICAP_URI = Scheme ":" Net_Path [ "?" Query ]
Scheme = "icap"
Net_Path = "//" Authority [ Abs_Path ]
Authority = [ userinfo "@" ] host [ ":" port ]
```

The request line specifies the ICAP resource that is being requested. Header fields follow with information, such as cache control and preview size. The header fields end with a blank line followed by the message body. The message body contains the encapsulated HTTP message sections that are being sent for scanning and modification.

Table 3-2 lists the request headers that are allowed in ICAP requests.

Table 3-2 Request headers

Header	Description
Allow	Lists the methods that the resource supports. For example, a client request can include an Allow: 204 header, which indicates that it will allow the server to reply to the message with a 204 No Content response if the file does not need modification. The client must buffer the message.
From	Provides the Internet email address for the user who is sending the client request. The address should use the standard HTTP mailbox format. For example: From: username@symantecdomain.com
Host	Specifies the host name and port number of the resource being requested.
Referer	Specifies the path that the client followed to obtain the URI. This optional header lets the server generate lists of backwards navigation links to resources and trace invalid links.
User-Agent	Identifies the software program that is used by the client that originated the request. This information is used for statistical purposes, to trace protocol violations, and to tailor responses to the software capabilities.
Preview (ICAP-specific header)	Lets the client send a portion of a file to Symantec Protection Engine for scanning. The client uses this header to specify the amount of data, in bytes, that will be sent for preview.

Table 3-2 Request headers *(continued)*

Header	Description
Encapsulated	Lists offsets of the start of each encapsulated section from the start of the message body. Opt-body=0 indicates filtering categories will be returned. See "About encapsulated messages" on page 30.
X-Filepath	Specifies the full file path to a local file.
X-URL-Blocked-Domain	This header is an optional field for a URL filtering request. This header is sent only when a URL is blocked at the domain level. For example, if Symantec Protection Engine is configured to block uninvitedads.com, then all URL scanning requests from uninvitedads.com domain receive this header in the ICAP response URL filtering requests are identified by following ICAP services: ■ SYMCScanReq-URL ■ SYMCScanReq-AV-URL ■ SYMCScanReqEx-AV-URL

Table 3-2 Request headers *(continued)*

Header	Description
X-Insight-Input-Info	This header is used for providing inputs for reputation scanning. You can have only one extended header for all input parameters. The value of this header is a comma separated list of key-value pair. For example: `X-Insight-Input-Info =‘DisableInsightCall=1, MD5FileHash=<md5 hash of the file>, SHA256FileHash=<SHA256 of file>,InsightAggressionLevel=1/2/3, IsDigitallySigned=0/1, ReportInsightInfo=0/1, SourceURL=<Source URL of the file>, SourceIP=<Source IP of the file>'`
	`DisableInsightCall` You can use this option to disable the query to Insight . ■ If DisableInsightCall is set to 1, all other Insight specific parameters are ignored. ■ If Insight is disabled at Symantec Protection Engine, there is no Insight query irrespective of the value of this parameter
	`InsightAggressionLevel` You can use this option to set the insight aggression level. The values are as follows: ■ 1: Low Insight aggression level. Hence, very less possibility of false positive detection. ■ 2: Medium Insight aggression level. ■ 3: High Insight aggression level. Hence, chances are there for false positive detection.
	`IsDigitallySigned` You can set the value in this option to enable/disable the extract of digital signing information of a file.The values are as follows: ■ 0: Does not extract the digital signing information of a file. ■ 1: Extracts the digital signing information of a file and uses it for Insight query. By default, Symantec Protection Engine assumes the file is signed.

Table 3-2 Request headers *(continued)*

Header	Description
	`ReportInsightInfo` You can set the value in this option to enable/disable reputation information in ICAP response. The values are as follows: ■ 0: Symantec Protection Engine does not provide reputation information in ICAP response. ■ 1: Symantec Protection Engine provides reputation information in ICAP response for Insight convicted files. **Note:**If provided, this parameter overrides the Symantec Protection Engine settings for EnableReputationInfo
	`MD5FileHash` You can provide the MD5 hash value of the file.
	`SHA256FileHash` You can provide the SHA256 value of the file.
	`SourceURL` You can provide the Source URL of the file.
	`SourceIP` You can provide the Source IP of the file.

About ICAP methods

Symantec Protection Engine supports the following ICAP methods:

OPTIONS (options mode)

Lets the client obtain information from an ICAP server about available services.

See “How to determine which services are supported (OPTIONS)” on page 40.

REQMOD (request modification mode)

Lets the client send URLs to Symantec Protection Engine for scanning services.

In request modification mode, the ICAP client receives a request from a user, usually a Web-browser. The client passes the data to Symantec Protection Engine for evaluation and processing.

See “Scanning HTTP requests (REQMOD)” on page 57.

RESPMOD (response modification mode)	Lets the client send files to Symantec Protection Engine for scanning services. In response modification mode, the ICAP client receives a data response from an origin server. The client passes the data to Symantec Protection Engine for evaluation and post-processing. See "Scanning HTTP responses (RESPMOD)" on page 66.
FILEMOD (file modification mode)	Lets the client pass a file name and path to Symantec Protection Engine so that Symantec Protection Engine can scan the file in place (rather than streaming the file to Symantec Protection Engine for scanning). **Note:** File modification mode deviates from the ICAP 1.0 specification that is presented in RFC 3507 (April 2003). See "Scanning non-HTTP data (RESPMOD and FILEMOD)" on page 71.

About ICAP services

Symantec Protection Engine supports antivirus and URL filtering scanning. You must include an ICAP service name in the ICAP URI to specify the type of scanning that you want Symantec Protection Engine to perform. Previous versions of Symantec AntiVirus Scan Engine used a different ICAP service naming convention. These services are supported for backward compatibility. New clients should use the new services, which include enhancements over the previous services.

Table 3-3 describes the ICAP services, descriptions, and the supported methods.

Table 3-3 ICAP services

ICAP service name	Description	Method options	Legacy or New service
AVSCANREQ	Lets you apply antivirus scanning to client request data (compatible with Symantec AntiVirus Scan Engine)	REQMOD	Legacy
AVSCANRESP	Lets you apply antivirus scanning to client response data (compatible with Symantec AntiVirus Scan Engine)	RESPMOD, FILEMOD	Legacy
AVSCAN	Lets you apply antivirus scanning to client response data	RESPMOD, FILEMOD	Legacy
SYMCScanReq-AV	HTTP request is provided to Symantec Protection Engine for antivirus scanning	REQMOD	Legacy

Table 3-3 ICAP services *(continued)*

ICAP service name	Description	Method options	Legacy or New service
SYMCScanReq-AV-URL	HTTP request is provided to Symantec Protection Engine for antivirus and URL-filtering scanning	REQMOD	Legacy
SYMCScanReq-URL	HTTP request is provided to Symantec Protection Engine for URL-filtering scanning	REQMOD	Legacy
SYMCScanResp-AV	HTTP response is provided to Symantec Protection Engine for antivirus scanning	RESPMOD, FILEMOD	Legacy
SYMCScanRespEx-AV	HTTP response is provided to Symantec Protection Engine for antivirus scanning, with enhanced threat categorization feature and Symantec Insight™ feature.	RESPMOD FILEMOD	New
SYMCScanReqEx-AV	HTTP request is provided to Symantec Protection Engine for antivirus scanning, with enhanced threat categorization feature and Symantec Insight™ feature.	REQMOD	New
SYMCScanReqEx-AV-URL	HTTP request is provided to Symantec Protection Engine for antivirus (with enhanced threat categorization feature), URL-filtering scanning, and Symantec Insight™ feature.	REQMOD	New

The ICAP service argument is used to specify the antivirus scanning policy. The action=repairpolicy argument can override the antivirus scanning repair policy for Symantec Protection Engine. For services that do not perform antivirus scanning, SYMCScanReq-URL and SYMCScanResp-DDR, the argument is ignored. The ICAP service argument is as follows:

action=repairpolicy

where repair policy consists of any of the following:

- scanrepairdelete
- scanrepair
- scandelete
- scan

You can append the argument to the service name by adding a question mark and then the argument. For example:

```
SYMCSCANRESP-AV?action=scanrepairdelete
```

About ICAP responses

ICAP client responses start with a status line, which includes the ICAP version and a status or response code. For example:

```
ICAP/1.0 200 OK
```

Following is the list of response codes that Symantec Protection Engine uses (response codes vary depending on the type of request).

- 100 Continue.
- 200 OK.
- 201 Created.
- 204 No content necessary.
- 400 Bad request.
- 403 Forbidden. Infected and not repaired.
- 404 Not found.
- 500 Internal server error.
- 502 Bad gateway.
- 505 ICAP version not supported.
- 506 Server too busy.
- 551 Resource unavailable.
- 558 Aborted - no scanning license.

The status line is followed by one or more response headers that let the server pass additional information (for example, information that cannot be placed in the status line) to the client.

Table 3-4 lists the response headers that Symantec Protection Engine uses (response headers vary depending on the type of request).

Table 3-4 Response headers

Header	Description
Date	Specifies the date and time as set on the server clock.
Service	Specifies the name and version number of the ICAP server.
Server-ID	Specifies the service requested.

Table 3-4 Response headers *(continued)*

Header	Description
ISTag (ICAP service tag)	Lets an ICAP server send service-specific information to an ICAP client. This data can be used to validate whether a server response, including cached data, is still valid. Symantec Protection Engine returns an ISTag with every response to indicate the state of the service, including all relevant configuration options and scanning definitions. Cached data that does not match the current ISTag is no longer valid. The value is a 32-character hexadecimal string. For example: ISTag: "B3C20CFCACEDA72CF16F6AEC119B2981"
Methods	Specifies the methods that are supported by the service that you queried.
Allow	Lists the optional ICAP features that the server supports.
Preview	Indicates the number of bytes of data that should be sent to Symantec Protection Engine for preview.
Transfer-Preview	Lists the file extensions that should be sent to Symantec Protection Engine for preview before sending the entire file. An asterisk (*) wildcard character represents the default behavior for all file extensions that are not specified in another transfer-type header.
Transfer-Complete	Lists the file extensions that should always be sent in their entirety to Symantec Protection Engine and that should not be previewed. An asterisk (*) wildcard character represents the default behavior for all file extensions that are not specified in another Transfer-type header.
Max-Connections	Indicates the maximum number of simultaneous ICAP connections that the server supports.
Options-TTL	Indicates the time (in seconds) during which the response is valid or cached. A blank header indicates that the response does not expire.
Encapsulated	Lists offsets of the start of each encapsulated section from the start of the message body.
X-AV-License	Indicates whether a valid antivirus scanning license is installed on Symantec Protection Engine, where 1 indicates a valid antivirus scanning license and 0 indicates no valid antivirus scanning license. The X-AV-License header does not include whether a URL filtering license is installed or valid.

Table 3-4 Response headers *(continued)*

Header	Description
X-Allow-Out	Indicates the custom X-headers that are returned in responses from Symantec Protection Engine.
X-Definition-Info	Indicates the date and revision number of the virus definitions in the following format: YYYYMMDD.RRR where YYYY is the four-digit year, MM is the month, DD is the day, and RRR is the revision number.
Opt-Body-Type	Indicates opt-body will be an attribute list. The attribute list begins with the following: X-ICAP-Attribute-<serviceid> This tag indicates that the start of the category list begins after this CRLF delimited header. The list contains the valid categories for the requested Service-ID. A semi-colon (;) followed by a blank line indicates the end of the list.
X-Outer-Container-Is-Mime	(Optional header) An integer value that indicates whether the outer container is a valid MIME container. A client application can use this information to reject content that does not meet this criteria. Zero (0) indicates that the outer container is not a valid MIME container, and one (1) indicates that the outer container is a valid MIME container.

Table 3-4 Response headers *(continued)*

Header	Description
X-Infection-Found	Provides information about an infection that is found. Only one violation is reported, regardless of the number of violations found. The header provides the following information regarding the infection: ■ Violation type An integer value for the violation. Zero (0) indicates a virus, one (1) indicates a mail policy violation, and two (2) indicates a container violation or malformity. ■ Resolution An integer value that indicates what action was taken on the file. Zero (0) indicates that the file was not fixed, one (1) indicates that the file was repaired, and two (2) indicates that access to the file was blocked. ■ Threat value String that describes the virus or violation that was found. This header applies to legacy services only. See "About ICAP services" on page 23.
X-Violations-Found	Indicates the total number of violations (either an infection or a policy violation) that were found in the scanned data. If violations were detected, the header is followed by a series of indented lines that provide the following information for each violation: ■ File name The name of the scanned file or the name of a nested component within the scanned file. Each component name is separated by a forward slash mark (/). ■ Violation name The English-readable name of the violation. ■ Violation ID A numeric code for the violation. ■ Disposition An integer value that indicates what action was taken to fix the file. Zero (0) indicates that the file was not fixed, one (1) indicates that the file was repaired, and two (2) indicates that the file was deleted.

Table 3-4 Response headers *(continued)*

Header	Description
X-URL-Blocked-Domain	Specifies the domain name for a URL request that Symantec Protection Engine has blocked. This header is an optional field for a URL filtering request. This header is sent only when a URL is blocked at the domain level. For example, if Symantec Protection Engine is configured to block uninvitedads.com, then all URL scanning requests from uninvitedads.com domain receive this header in the ICAP response. URL filtering requests are identified by following ICAP services: ■ SYMCScanReq-URL ■ SYMCScanReq-AV-URL ■ SYMCScanReqEx-AV-URL
X-File-Insight-Info	Indicates the number of files, for which there is Insight related information available. This response header will have following parameters **1) InsightResult :** ■ 1: Indicates that the file is detected/convicted by Insight and the reputation information for the file is available. ■ 2: Indicates network timeout during an Insight query. In such cases Insight information of file is not available. ■ 3: Indicates that Insight information of file is unknown due to some reason. ■ 4: Indicates that license for Insight is not available. ■ 5: Indicates that there was a scan error during an Insight query. **Note:** : Below parameters will not appear if InsightResult value is other than 1 **2) Reputation:**Reputation status for a file. **3) Age :** Age of the file. **4) Prevalence:** The prevalence information for a file. **5) True type:** The type of the file. **6) SHA256:** SHA256 hash value of the file.
X-Insight-License	Indicates whether a valid Insight scanning license is installed on Symantec Protection Engine, where 1 indicates a valid Insight scanning license and 0 indicates no valid Insight scanning license.

Table 3-4 Response headers *(continued)*

Header	Description
X-Insight-Cache-Revocation-Content	Indicates the date and revision number of the Insight cache revocation content definitions in the following format: YYYYMMDD.RRR where YYYY is the four-digit year, MM is the month, DD is the day, and RRR is the revision number.
X-Insight-Threshold-Setting-Content	Indicates the date and revision number of the Insight threshold setting content definitions in the following format: YYYYMMDD.RRR where YYYY is the four-digit year, MM is the month, DD is the day, and RRR is the revision number.
X-Insight-symVT-Content	Indicates the date and revision number of the Insight symVT content definitions in the following format: YYYYMMDD.RRR where YYYY is the four-digit year, MM is the month, DD is the day, and RRR is the revision number.
X-APK-Reputation-Info	Indicates the APK error code that caused the APK reputation query failure. "X-APK-Reputation-Info" extended header will be present in ICAP scan result only if one of the below mentioned scenario occurs during APK file scanning provided APK reputation is enabled at Symantec Protection Engine. ■ No APK reputation feature license at Symantec Protection Engine. ■ Symantec Protection Engine’s APK scanner is overloaded. ■ Some error occurred during APK file scanning. Example of APK result code in ICAP response is shown below ■ X-APK-Reputation-Info: 1 <Number of APK reputation query failure> ■ apk10.apk : <Name of the APK file for which the reputation query failed> ■ APKResult=21 <APK result code that caused the query failure>

About encapsulated messages

The ICAP encapsulation model provides a lightweight means of packaging multiple HTTP message sections into a single ICAP message for vectoring of requests, responses, and request/response pairs on an ICAP server. An encapsulated section can consist of HTTP message headers and bodies.

Encapsulated HTTP message bodies must be transferred using chunked transfer encoding. This keeps the transport-layer connection between the client and server open for later use and lets the server send incremental responses to reduce the latency that is perceived by users. Encapsulated HTTP headers are not chunked. This lets the ICAP client copy the header directly from the HTTP client to the ICAP server without having to reprocess it.

Note: The chunked transfer encoding modifies the body of a message so that it can be transferred as a series of chunks, each with its own (hexadecimal) size indicator, followed by an optional footer that contains entity-header fields. For more information, see the HTTP/1.1 specification (RFC 2616, section 3.6.1).

The encapsulated header must be included in every ICAP message, except for OPTIONS requests. This header provides information about where each encapsulated section and message body starts and ends.

For example:

```
Encapsulated: req-hdr=0, res-hdr=45, res-body=100
```

This example indicates that the message encapsulates a group of request headers, response headers, and a response body at 0, 45, and 100 byte offsets. Byte offsets use a decimal format. Chunk sizes within an encapsulated body use a hexadecimal format. If no message body is sent, a null-body entity is used.

Encapsulated headers use the following syntax:

```
encapsulated_header: "Encapsulated: " encapsulated_list
encapsulated_list: encapsulated_entity |
      encapsulated_entity ", " encapsulated_list
encapsulated_entity: reqhdr | reshdr | reqbody | resbody | optbody
reqhdr  = "req-hdr" "=" (decimal integer)
reshdr  = "res-hdr" "=" (decimal integer)
reqbody = { "req-body" | "null-body" } "=" (decimal integer)
resbody = { "res-body" | "null-body" } "=" (decimal integer)
optbody = { "opt-body" | "null-body" } "=" (decimal integer)
```

Encapsulated headers must end with a blank line to make them readable and to terminate line-by-line HTTP parsers.

Where to find more information on ICAP

Symantec Protection Engine supports the ICAP 1.0 specification that is presented in RFC 3507 (April 2003). Much of the information in the *Symantec Protection Engine Software Developer's Guide* is obtained directly from the specification. However, the specification contains more extensive examples and additional information. Developers are encouraged to consult the specification, as well as other sources.

For more information about ICAP specifications, go the following URL:

http://www.icap-forum.org

The URL filtering feature was implemented using the ICAP Extensions Internet Draft, section 5.2.

About the scanning process

Symantec Protection Engine provides antivirus and URL-filtering scanning services to ICAP clients.

The scanning services are provided for non-HTTP scanning, such as email and FTP traffic, and the following user scenarios:

- A user requests a file from a Web site
- A user posts a file to a Web site
- A user receives a file from a Web site

When an ICAP client receives an HTTP request, it is encapsulated into an ICAP REQMOD request and sent to a protection engine ICAP service. The service that is specified in the URI must support the REQMOD method. This is a simple request with HTTP request headers and no body. Because there is no data to scan for viruses, there is no value added by an antivirus-only service like SYMCScanReq-AV. The other REQMOD services, SYMCScanReq-URL, SYMCScanReq-AV-URL and SYMCScanReqEx-AV-URL, will do the same.

If an HTTP request contains a file, such as a posting to a Web site, there is value to antivirus scanning. Symantec Protection Engine can either repair the file (return a modified HTTP request) or notify the user (return an HTTP response), but not both. Therefore, for REQMOD antivirus scanning, the file is never repaired (scanpolicy = scan). The user receives a Web page that states that the post failed because the file was infected or triggered another violation.

When an ICAP client receives an HTTP response from an origin server, it is encapsulated into an ICAP RESPMOD request and sent to Symantec Protection Engine. The service specified must support RESPMOD. The service specified determines the kind of scanning that is performed on the HTTP body: antivirus, URL filtering, or both. Because Symantec Protection Engine has an option to ignore the URL filtering results based on the URL, Symantec Protection Engine must also scan the URL in the HTTP request headers.

The ICAP RFC specifies that these headers are optional for a response modification request, but for clients that use Symantec Protection Engine, they are required. It is possible to get URL filtering on a RESPMOD request, but it is more efficient to block URLs during the request before expending resources to retrieve the data.

Symantec Protection Engine can be used to scan non-HTTP data, such as files on disk, email messages, and FTP traffic. You can scan non-HTTP data by creating an ICAP RESPMOD request with a minimal set of fabricated HTTP request headers and HTTP response headers. Typically the HTTP request headers include an HTTP request line that contains the file name (Symantec Protection Engine provides features based on file name, so this is required) and a Host header. The HTTP response headers contain an HTTP response line: HTTP/1.1 200 OK.

Symantec Protection Engine also supports an extension to ICAP (FILEMOD), which lets the client send a request to have a file scanned on-disk to avoid sending the file across the network. An ICAP client requests on-disk scanning by sending an ICAP FILEMOD request to Symantec Protection Engine. This request is composed of ICAP headers only and no ICAP body (Encapsulated: null-body=0). Included in the headers is the path that Symantec Protection Engine can use to access the file. The ICAP response will be similar to a network scan, except that no data will be returned. Any modification is done on the actual file.

Before sending ICAP requests, the client can query the ICAP server by using the OPTIONS method to determine which services are supported.

See “How to determine which services are supported (OPTIONS)” on page 40.

About scanning URLs

When scanning URLs, the URL can be constructed in the following ways:

When the HTTP request line contains only the path information, it is combined with the host name that is provided in the Host header to create the full URL.	GET/directory/file.exe HTTP/1.1 Host: client.symantecdomain.com The URL is client.symantecdomain.com/directory/file.exe
The URL can also be sent completely in the HTTP request line. This is typically the case for HTTP POST requests.	POST http://client.symantecdomain.com/directory/file.exe HTTP/1.1 Host: client.symantecdomain.com The URL is extracted from the request line and the Host header is ignored.

About sending files for scanning

Symantec Protection Engine supports multiple URIs for scanning services. The URI uses the following format:

```
icap://server.name:port/servicename
```

where server.name is the name of the server on which Symantec Protection Engine is running. The port number is optional if Symantec Protection Engine is running on port 1344, which is the default ICAP port. Servicename is one of the ICAP services.

See "About ICAP services" on page 23.

About sending portions of files for preview

Symantec Protection Engine can preview data to determine whether it needs to be scanned based on known virus behavior. For example, .gif files are typically not scanned because they generally do not contain executable code. The rules for which types of files are suitable for preview are determined by the exclusion lists that are configured in the policy.xml and the x-path for same is `//policies/ThreatPolicies/ ExcludeList/`

Before a file is sent for scanning, the client should send an OPTIONS request to determine whether a file type is suitable for preview and how much data should be sent.

Symantec Protection Engine provides this information in the following headers of the OPTIONS response message:

Preview	Indicates the preferred number of bytes of data that can be sent
Transfer-Complete	Indicates which file types should be sent in their entirety
Transfer-Preview	Indicates which file types should be sent for preview

See "How to determine which services are supported (OPTIONS)" on page 40.

Table 3-5 details Symantec Protection Engine scanning behavior that is based on the scanning policies that you configure.

Table 3-5 Scanning behavior

Scanning policy	Transfer-Complete header	Transfer-Preview header	Scanning behavior
Previews all files	Not used	Asterisk (*) character	All files are previewed for unwanted content.
Scan all files regardless of extension	Asterisk (*) character	Not used	Symantec Protection Engine scans every file in its entirety without previewing it first.

Table 3-5 Scanning behavior *(continued)*

Scanning policy	Transfer-Complete header	Transfer-Preview header	Scanning behavior
Scan all files except those with the following extensions (exclusion list)	Asterisk (*) character	List of file extensions	Symantec Protection Engine previews the file types that are listed in the Transfer-Preview header for unwanted content. All other file types, including unidentified file types, are scanned in their entirety.

For more information, see the *Symantec Protection Engine Implementation Guide*.

If an OPTIONS response indicates that a file is suitable for preview, the client should include a Preview header in the request message that indicates the portion of data, in bytes, that is being sent for preview. Symantec Protection Engine evaluates the initial chunk of data to determine whether a full scan is required. If so, Symantec Protection Engine requests the remainder of the data. Scan results are returned in the RESPMOD response message.

About allowing No Content responses

The Allow: 204 header is an optional request header that lets Symantec Protection Engine return a 204 No Content response code if the message does not require modification. This can optimize server performance because Symantec Protection Engine can determine whether a file is uninfected without having to receive the entire message, and Symantec Protection Engine does not have to return a message. The processing burden is placed on the client, which must buffer the entire message during the scan. Symantec Protection Engine returns a 204 No Content response outside of a preview only if the client request includes an Allow: 204 header.

About threat category responses

When Symantec Protection Engine detects a viral or non-viral threat during a scan using services like SYMCScanReqEx-AV, SYMCScanRespEx-AV and SYMCScanReqEx-AV-URL, the ICAP X-Violations-Found response header has additional enhanced threat categorization information about the threat which includes the following:

- Threat category name (ViralThreat or NonViralThreat)
- SubCategory ID
- Uber Categories

- Cumulative Risk Rating
- Performance Impact
- Privacy Impact
- Ease Of Removal
- Stealth
- Subcategory description

All the extended threat information is appended to the virus name with a delimiter pipe. To be able to obtain this extended threat categorization information, the following parameters need to be enabled in configuration.xml on the Symantec Protection Engine:

- EnableThreatCategoryInformation
- EnableSubCategoryDescriptionResp

Refer to the Symantec Protection Engine Implementation Guide for more details.

An example of an X-Violations-Found response header with a Threat category is as follows:

```
C: RESPMOD icap://127.0.0.1:1344/SYMCScanRespEx-AV ICAP/1.0
C: Host: 127.0.0.1:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=52, res-body=71
C:
C: get eicar.com HTTP/1.1
C: Host:icheck.symantec.com
C:
C: HTTP/1.1 200 OK
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "44C5020856436B4C8FF7F8EA9F287653"
S: Date: Tue Jul 24 17:19:58 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.44
S: Service-ID: SYMCSCANRESPEX-AV
S: X-Violations-Found: 1
S: eicar.com
S: EICAR Test String| ViralThreat=Virus| SubCategoryID=0|
UberCategories=Malware| CumulativeRiskRating=High|
PerformanceImpact=High| PrivacyImpact=High|
EaseOfRemoval=High| Stealth=High|
SubCategoryDescription=Programs that infect other programs,
files, or areas of a computer by inserting themselves or
attaching themselves to that medium.
S: 11101
S: 2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=83
```

See “About ICAP responses” on page 25.

About non-viral threat category responses

Previously, when Symantec Scan Engine detects a non-viral threat during a scan, the ICAP X-Violations-Found response header includes the threat category name (NonViralThreat) in the Threat Description field. The threat category name is appended to the virus name with a delimiter pipe. For example, ThreatDescription= <VirusName> | NonViralThreat=<CategoryName>.

From Symantec Protection Engine 7.x and C API 7.x onwards, this legacy behavior will be applicable only if legacy services (SYMCScanReqEx* and SYMCScanRespEx* are the new services) are used for scanning.

The following is a list of all the values currently supported for categories for non-viral threats (with legacy services):

- Adware
- Spyware
- Reserved Malicious
- Malicious
- Heuristic
- Hack Tools
- Trackware
- Dialers
- Joke Programs
- Remote Access
- Security Risks

By default, Symantec Protection Engine does not send the threat category name in the header. To configure Symantec Protection Engine to send the threat category name, you must change the EnableNonViralThreatCategoryResp value in the configuration.xml file to true. For more information about how to modify the configuration.xml file using theXMLmodifier command-line tool, see the *Symantec Protection Engine Implementation Guide*.

An example of an X-Violations-Found response header with a NonViralTreat category is as follows:

```
C: RESPMOD icap://127.0.0.1:1344/SYMCScanResp-AV ICAP/1.0
C: Host: 127.0.0.1:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=44, res-body=63
C:
C: get / HTTP/1.1
C: Host:icheck.symantec.com
C:
C: HTTP/1.1 200 OK
C:
S: ICAP/1.0 201 Created
ISTag: "C5D8B6B34BC2785CE5017A242480E9C2"
Date: Sun May 20 05:10:32 2012 GMT
Service: Symantec Protection Engine/7.0.0.31
Service-ID: SYMCSCANRESP-AV
X-Violations-Found: 1
index.html
Adware.Unknown| NonViralThreat=Adware
4294909841
2
X-Outer-Container-Is-Mime: 0
Encapsulated: res-hdr=0, res-body=83
```

About file Insight information

A new ICAP extended header X-File-Insight-Info is introduced to indicate the reputation information for a file. This ICAP header is applicable only if the Symantec Insight™ feature is enabled.

The X-File-Insight-Info response header in ICAP response is driven by the EnableReputationInfo parameter in the configuration.xml file.

Table 3-6 lists the X-File-Insight-Info header parameters.

Table 3-6 Parameters for X-File-Insight-Info ICAP header

Parameter	Description
InsightResult	This paramter hasthe following values: ■ 1: Indicates that the file is detected/convicted by Insight and the reputation information for the file is available. ■ 2: Indicates network timeout during an Insight query. In such cases, Insight information of file is not available. ■ 3: Indicates that Insight information of file is unknown due to some reason. ■ 4: Indicates that Insight license is not available. ■ 5: Indicates that there was a scan error during the Insight query.
Reputation	Reputation status for a file.
Age	Age of the file.
Prevalence	The prevalence information for a file.
True type	The type of the file.
SHA256	SHA256 hash value of the file.

About APK reputation information

Indicates the APK error code that caused the APK reputation query failure. "X-APK-Reputation-Info" extended header will be present in ICAP scan result only if one of the below mentioned scenario occurs during APK file scanning provided APK reputation is enabled at SPE

- No APK reputation feature license at Symantec Protection Engine
- Symantec Protection Engine’s APK scanner is overloaded.
- Some error occurred during APK file scanning

Example of APK result code in ICAP response is shown below

- X-APK-Reputation-Info: 1 <Number of APK reputation query failure>
- apk10.apk : <Name of the APK file for which the reputation query failed>
- APKResult=21 <APK result code that caused the query failure>

Table 3-7 lists the X-APK-Reputation-Info header parameters.

Table 3-7 Parameters for X-APK-Reputation-Info ICAP header

Parameter	Description
APKResult	This paramter has the following values: ■ The APK result code will indicate the error that has occured when APK file is scanned.

How to determine which services are supported (OPTIONS)

The OPTIONS method lets a client application query an ICAP server for information about supported services and commands and preferred file handling methods. The client application should perform this query before sending files for scanning.

The OPTIONS method consists of a request line that contains the URI for the Symantec Protection Engine service that you want to query.

When Symantec Protection Engine receives an OPTIONS request from a client application, it sends a response that includes the following information:

- Maximum number of simultaneous connections allowed
- Preferred data preview size
- Preferred file handling methods
- Supported methods (REQMOD, RESPMOD, FILEMOD)
- For URL filtering services, the list of URL categories that are available is returned in an encapsulated opt-body section
  See "About licensing" on page 11.

See "About ICAP responses" on page 25.

About using the OPTIONS request to determine if the server is overloaded

If you use ICAP, the ICAP threshold client notification feature is enabled by default. When the number of queued requests for a Symantec Protection Engine exceeds its threshold, Symantec Protection Engine rejects the scan request. It notifies the client that the server has reached the queued request threshold. The client can then adjust the load balancing, which prevents the server from being overloaded with scan requests. This feature lets the client applications that pass files to Symantec Protection Engine benefit from load-balanced scanning without any additional effort.

You can use the OPTIONS request to determine if Symantec Protection Engine is overloaded. Send an OPTIONS request to the Symantec Protection Engine. If Symantec Protection Engine is not busy, it will send the standard OPTIONS response to the connector and will keep the connection open. If Symantec Protection Engine is too busy to process the request, it will reply with 506 response “Server too busy” and will close the connection. In this case, the load balancing decision should be made by the connector.

A sample ICAP response body for code 506 is as follows:

```
ICAP/1.0 506 Server too busy
ISTag: "638FC09D7F7CCFD3DCF0E659FFEAD53F"
Date: Sun May 20 05:10:32 2012 GMT
Service: Symantec Protection Engine/7.0.0.31
Service-ID: Respmod AV Scan
```

About querying antivirus-only services

The antivirus-only services include the following:

AVSCAN

Provides antivirus scanning for HTTP requests.

The request must include a file (uploading) and use the HTTP POST method. Otherwise, an ICAP 200 OK response is returned.

This is a legacy service and should not be used by new clients.

AVSCANREQ

Provides antivirus scanning for HTTP requests.

The request must include a file (uploading) and use the HTTP POST method. Otherwise, an ICAP 200 OK response is returned.

This is a legacy service and should not be used by new clients.

AVSCANRESP

Provides antivirus scanning for HTTP requests.

The request must include a file (uploading) and use the HTTP POST method. Otherwise, an ICAP 200 OK response is returned.

This is a legacy service and should not be used by new clients.

SYMScanReq-AV

Provides antivirus scanning for HTTP requests.

The request must include a file (uploading) and use the HTTP POST method. Otherwise, an ICAP 200 OK response is returned.

SYMCScanResp-AV

Provides antivirus scanning for content that is downloaded from the Internet.

SYMCScanRespEx-AV

HTTP response is provided to Symantec Protection Engine for antivirus scanning.

SYMCScanReqEx-AV

HTTP request is provided to Symantec Protection Engine for antivirus scanning
.

An OPTIONS request to an antivirus-only service provides the validity of the antivirus license, the antivirus definitions version, and an ISTag, which indicates the state of the configuration settings.

See "About licensing" on page 11.

ICAP services lists the services that you can use for scan, repair, and delete functions. You must have a valid license installed to perform scanning functions.

See "About ICAP services" on page 23.

Examples of OPTIONS requests for antivirus scanning are as follows:

```
/* AV is only performed on POST requests */
OPTIONS icap://icapclient.sse.com/symcscanreq-url ICAP/1.0
Host: icapclient.sse.com
```

About querying URL filtering services

The URL filtering services include the following:

SYMCScanReq-URL

Blocks requests to sites based on the URL.

This includes comparing the requested URL to Symantec's URL category lists, Child Abuse Image Content (CAIC) category lists, and user defined Local category lists.

For more information about how URL filtering works, see the *Symantec Protection Engine Implementation Guide*.

Examples of OPTIONS requests for URL filtering are as follows:

```
OPTIONS icap://sse.com/symcscanreq-url ICAP/1.0
Host: icapclient.sse.com
```

About querying antivirus and URL filtering services

The antivirus and URL filtering scanning services include the following:

SYMCScanReq-AV-URL

Performs URL filtering on HTTP requests and scans HTTP bodies (files) for malicious content.

SYMCScanReqEx-AV-URL

HTTP request is provided to Symantec Protection Engine for antivirus (with enhanced threat categorization feature) and URL-filtering scanning

Examples of OPTIONS requests for antivirus and URL filtering are as follows:

```
/* AV is only performed on POST requests */
OPTIONS icap://sse.com/symcscanreq-av-url ICAP/1.0
Host: icapclient.sse.com
```

OPTIONS examples

Examples of OPTIONS services are as follows:

- OPTIONS antivirus-scanning example
- OPTIONS URL filtering scanning example
- OPTIONS antivirus and URL filtering scanning example

OPTIONS antivirus-scanning example

The antivirus scanning services perform scanning, repair, and delete functions by using the scanning preferences that you specify through the Symantec Protection Engine policies.

Use the following format to specify the URI:

```
icap://<Server>/<service>
```

A sample OPTIONS request on SYMCScanReq-AV is as follows:

```
C: OPTIONS icap://172.16.11.19:1344/SYMCScanReq-AV ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Mon Apr 23 08:07:30 2012 GMT
S: Methods: REQMOD
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQ-AV
S: ISTag: "DBDF573DB137CC3FD88B5C294F14427F"
S: X-Definition-Info: 20120418.002
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime,
   X-Infection-Found,
S: X-Allow-Out: X-Definition-Info, X-AV-License
S: X-Allow-Out: X-Violations-Found
S: Allow: 204
S: Options-TTL: 3600
```

```
S: Preview: 4
S: Transfer-Preview: *
S: X-AV-License: 1
S: Encapsulated: null-body=0
S:
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported method is REQMOD.
- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.
- The data in the response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
  The maximum number of simultaneous connections that Symantec Protection Engine supports varies on the operating environment.

A sample OPTIONS response on SYMCScanResp-AV is as follows:

```
C: OPTIONS icap://172.16.11.19:1344/SYMCScanResp-AV ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Sat Apr 21 07:30:10 2012 GMT
S: Methods: RESPMOD, FILEMOD
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-AV
S: ISTag: "DBDF573DB137CC3FD88B5C294F14427F"
S: X-Definition-Info: 20120418.002
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime,
   X-Infection-Found
S: X-Allow-Out: X-Definition-Info, X-AV-License
S: X-Allow-Out: X-Violations-Found
S: Allow: 204
S: Options-TTL: 3600
S: Preview: 4
S: Transfer-Preview: *
S: X-AV-License: 1
```

```
S: Encapsulated: null-body=0
S:
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported methods are RESPMOD and FILEMOD.
- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.
- The data in this response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
  The maximum number of simultaneous connections that Symantec Protection Engine supports varies on the operating environment.

A sample OPTIONS response on SYMCScanReqEx-AV is as follows:

```
OPTIONS icap://127.0.0.1:1344/SYMCScanReqEx-AV ICAP/1.0
C: Host: 10.219.209.99:1344
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Wed Jan 08 09:48:34 2014 GMT
S: Methods: REQMOD
S: Service: Symantec Protection Engine/7.5.0.32
S: Service-ID: SYMCSCANREQEX-AV
S: ISTag: "2C8F4CA6A9AECEA0737A046C2744231B"
S: X-Definition-Info: 20140107.041
S: X-Insight-Cache-Revocation-Content: 20140107.033
S: X-Insight-Threshold-Setting-Content: 20131211.009
S: X-Insight-symVT-Content: 20131125.019
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime, X-Infection-Found, X-Definition-Info, X-AV-
S: X-Allow-Out: X-Violations-Found
S: X-Allow-Out: X-File-Insight-Info, X-Insight-Cache-Revocation-Content, X-Insight-Thr
S: Allow: 204
S: Options-TTL: 3600
S: Preview: 4
S: Transfer-Preview: *
S: X-AV-License: 1
S: X-Insight-License: 1
S: Encapsulated: null-body=0
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported method is REQMOD.
- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.
- The data in the response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
  The maximum number of simultaneous connections that Symantec Protection Engine supports varies on the operating environment.

A sample OPTIONS response on SYMCScanRespEx-AV is as follows:

```
OPTIONS icap://10.219.209.99:1344/SYMCScanRespEx-AV ICAP/1.0
C: Host: 10.219.209.99:1344
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Wed Jan 08 09:45:08 2014 GMT
S: Methods: RESPMOD, FILEMOD
S: Service: Symantec Protection Engine/7.5.0.32
S: Service-ID: SYMCSCANRESPEX-AV
S: ISTag: "2C8F4CA6A9AECEA0737A046C2744231B"
S: X-Definition-Info: 20140107.041
S: X-Insight-Cache-Revocation-Content: 20140107.033
S: X-Insight-Threshold-Setting-Content: 20131211.009
S: X-Insight-symVT-Content: 20131125.019
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime, X-Infection-Found,
X-Definition-Info, X-AV-License
S: X-Allow-Out: X-Violations-Found
S: X-File-Insight-Info, X-Insight-Cache-Revocation-Content, X-Insight-Threshold-Settin
S: Allow: 204
S: Options-TTL: 3600
S: Preview: 4
S: Transfer-Preview: *
S: X-AV-License: 1
S: Encapsulated: null-body=0
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported methods are RESPMOD and FILEMOD.

- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.
- The data in this response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
- The maximum number of simultaneous connections that Symantec Protection Engine supports varies on the operating environment.

OPTIONS URL filtering scanning example

The URL filtering scanning services perform URL filtering based on the options that you specify in Symantec Protection Engine policies.

Use the following format to specify the URI:

```
icap://<Server>/<service>
```

A sample OPTIONS request on SYMCScanReq -URL is as follows:

```
C: OPTIONS icap://10.219.209.43:1344/SYMCScanReq-URL ICAP/1.0
C: Host: 10.219.209.43:1344
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Sat Apr 14 11:35:20 2016 GMT
S: Methods: REQMOD
S: Service: Symantec Protection Engine/7.8.0.140
S: Service-ID: SYMCSCANREQ-URL
S: ISTag: "2F44ECAE3480319155E7D315031F42EC"
S: X-Definition-Info: 20151216.022
S: X-SYMANTEC-URL-Definition-Info: 20100817.045
S: X-CAIC-URL-Definition-Info: 20100817.042
S: X-SYMANTEC-URLReputation-Definition-Info: 20160414.016
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime,X-Infection-Found, X-Definition-Info, X-AV-L
   X-Infection-Found, X-Definition-Info, X-AV-License
S: X-Allow-Out: X-URL-Blocked-Domain
S: X-Allow-Out: X-Violations-Found
S: Allow: 204
S: Options-TTL: 3600
S: Preview: 4
S: Transfer-Preview: *
```

```
S: X-AV-License: 1
S: Encapsulated: opt-body=0
S: X-Allow-Out: X-Attribute
S: Opt-Body-Type: Attribute-List
S:
S: 4c0
S: X-ICAP-Attribute-SYMCSCANREQ-URL
S: Abortion
S: Advertising
S: Alcohol
S: Anonymizer
S: Art and Museums
S: Art Nudes
S: Automated Web Application
S: Automotive
S: Bikini
S: Blog
S: Business
S: Business Wireless
S: CAIC
S: Cash Gambling
S: Chat
S: Chat/SMS/Text Messaging Wireless
S: Criminal Skills
S: Cults
S: Drugs
S: Dynamic
S: Dynamic Wireless
S: Education
S: Energy
S: Enterprise Webmail
S: Entertainment
S: Entertainment Wireless
S: File Sharing
S: Finance Wireless
S: Finance and Investing
S: Food and Restaurants
S: Forums and Message Boards
S: Freeware and Shareware
S: Gambling
S: Gambling Wireless
S: Gaming
S: Glamour
```

```
S: Gore
S: Government
S: Hacking
S: Hate
S: Health
S: Hobbies
S: Hosting
S: Internet Telephony
S: Job Search
S: Kids
S: Law
S: Lifestyle
S: Mature Content
S: Military
S: Mobile Entertainment
S: Music
S: News
S: News Wireless
S: Non profit
S: Occult
S: Personal Ads and Dating
S: Personal Ads andd Dating Wireless
S: Pets
S: Placeholder
S: Politics
S: Pornography
S: Pornography Wireless
S: Portal
S: Proxy Wireless
S: Real Estate
S: Reference
S: Religion
S: Science
S: Search
S: Self Harm
S: Sexual Education
S: Shopping
S: Sports
S: Sports Wireless
S: Streaming Media
S: Suicide
S: Technology and Telecommunications
S: Tobacco
```

```
S: Travel
S: Travel Wireless
S: Violence
S: Virtual Community
S: Weapons
S: Webmail
S: Wedding
S: AllowURLsCategory
S: URLReputation
S: ;
S:
S: 0
S:
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported method is REQMOD.
- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.
- The data in this response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
  The maximum number of simultaneous connections that Symantec Protection Engine supports varies depending on the operating environment.

You will see new information that starts with Encapsulated: opt-body=0. When scanning for content, an opt-body header is returned that indicates a list of categories that are supported by Symantec Protection Engine. X-Allow-Out contains an addition of X-Attribute and the Opt-Body-Type is Attribute-List.

OPTIONS antivirus and URL filtering scanning example

The SYMCScan* services perform antivirus scanning, repair, and delete functions and URL filtering based on the scanning preferences that you specify in Symantec Protection Engine policies.

Use the following format to specify the URL:

```
icap://<Server>/<service>
```

A sample OPTIONS request on SYMCScanReq-AV-URL is as follows:

```
C: OPTIONS icap://10.219.209.43:1344/SYMCScanReq-AV-URL ICAP/1.0
C: Host: 10.219.209.43:1344
```

```
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Sat Apr 14 11:39:56 2016 GMT
S: Methods: REQMOD
S: Service: Symantec Protection Engine/7.8.0.140
S: Service-ID: SYMCSCANREQ-AV-URL
S: ISTag: "6B94FB121ED0E2B412F0CF43E803F9DB"
S: X-Definition-Info: 20151216.022
S: X-SYMANTEC-URL-Definition-Info: 20100817.045
S: X-CAIC-URL-Definition-Info: 20100817.042
S: X-SYMANTEC-URLReputation-Definition-Info: 20160414.016
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime,  X-Infection-Found, X-Definition-Info, X-AV
   X-Infection-Found, X-Definition-Info, X-AV-License
S: X-Allow-Out: X-URL-Blocked-Domain
S: X-Allow-Out: X-Violations-Found
S: Allow: 204
S: Options-TTL: 3600
S: Preview: 4
S: Transfer-Preview: *
S: X-AV-License: 1
S: Encapsulated: opt-body=0
S: X-Allow-Out: X-Attribute
S: Opt-Body-Type: Attribute-List
S:
S: 4c3
S: X-ICAP-Attribute-SYMCSCANREQ-AV-URL
S: Abortion
S: Advertising
S: Alcohol
S: Anonymizer
S: Art and Museums
S: Art Nudes
S: Automated Web Application
S: Automotive
S: Bikini
S: Blog
S: Business
S: Business Wireless
S: CAIC
S: Cash Gambling
```

```
S: Chat
S: Chat/SMS/Text Messaging Wireless
S: Criminal Skills
S: Cults
S: Drugs
S: Dynamic
S: Dynamic Wireless
S: Education
S: Energy
S: Enterprise Webmail
S: Entertainment
S: Entertainment Wireless
S: File Sharing
S: Finance Wireless
S: Finance and Investing
S: Food and Restaurants
S: Forums and Message Boards
S: Freeware and Shareware
S: Gambling
S: Gambling Wireless
S: Gaming
S: Glamour
S: Gore
S: Government
S: Hacking
S: Hate
S: Health
S: Hobbies
S: Hosting
S: Internet Telephony
S: Job Search
S: Kids
S: Law
S: Lifestyle
S: Mature Content
S: Military
S: Mobile Entertainment
S: Music
S: News
S: News Wireless
S: Non profit
S: Occult
S: Personal Ads and Dating
```

```
S: Personal Ads andd Dating Wireless
S: Pets
S: Placeholder
S: Politics
S: Pornography
S: Pornography Wireless
S: Portal
S: Proxy Wireless
S: Real Estate
S: Reference
S: Religion
S: Science
S: Search
S: Self Harm
S: Sexual Education
S: Shopping
S: Sports
S: Sports Wireless
S: Streaming Media
S: Suicide
S: Technology and Telecommunications
S: Tobacco
S: Travel
S: Travel Wireless
S: Violence
S: Virtual Community
S: Weapons
S: Webmail
S: Wedding
S: AllowURLsCategory
S: URLReputation
S: ;
S:
S: 0
S:
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported method is REQMOD.
- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.

- The data in this response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
  The maximum number of simultaneous connections that Symantec Protection Engine supports varies on the operating environment.

You will see new information that starts with Encapsulated: opt-body=0. When scanning for content, an opt-body header is returned that indicates a list of categories that are supported by Symantec Protection Engine. X-Allow-Out contains an addition of X-Attribute and the Opt-Body-Type is Attribute-List.

A sample OPTIONS request on SYMCScanReqEx-AV-URL is as follows:

```
C: OPTIONS icap://10.219.209.43:1344/SYMCScanReqEx-AV-URL ICAP/1.0
C: Host: 10.219.209.43:1344
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 200 OK
S: Date: Sat Apr 14 11:43:20 2016 GMT
S: Methods: REQMOD
S: Service: Symantec Protection Engine/7.8.0.140
S: Service-ID: SYMCSCANREQEX-AV-URL
S: ISTag: "6B94FB121ED0E2B412F0CF43E803F9DB"
S: X-Definition-Info: 20151216.022
S: X-SYMANTEC-URL-Definition-Info: 20100817.045
S: X-CAIC-URL-Definition-Info: 20100817.042
S: X-SYMANTEC-URLReputation-Definition-Info: 20160414.016
S: X-Insight-Cache-Revocation-Content:  20160413.033
S: X-Insight-Threshold-Setting-Content: 20160125.017
S: X-Insight-symVT-Content: 20160412.005
S: Max-Connections: 128
S: X-Allow-Out: X-Outer-Container-Is-Mime, X-Infection-Found, X-Definition-Info, X-AV-
S  X-Infection-Found, X-Definition-Info, X-AV-License
S: X-Allow-Out: X-URL-Blocked-Domain
S: X-Allow-Out: X-Violations-Found
S: X-Allow-Out: X-File-Insight-Info, X-Insight-Cache-Revocation-Content, X-Insight-Thr
S: Allow: 204
S: Options-TTL: 3600
S: Preview: 4
S: Transfer-Preview: *
S: X-AV-License: 1
S: Encapsulated: opt-body=0
S: X-Allow-Out: X-Attribute
S: Opt-Body-Type: Attribute-List
```

```
S:
S: 4c5
S: X-ICAP-Attribute-SYMCSCANREQEX-AV-URL
S: Abortion
S: Advertising
S: Alcohol
S: Anonymizer
S: Art and Museums
S: Art Nudes
S: Automated Web Application
S: Automotive
S: Bikini
S: Blog
S: Business
S: Business Wireless
S: CAIC
S: Cash Gambling
S: Chat
S: Chat/SMS/Text Messaging Wireless
S: Criminal Skills
S: Cults
S: Drugs
S: Dynamic
S: Dynamic Wireless
S: Education
S: Energy
S: Enterprise Webmail
S: Entertainment
S: Entertainment Wireless
S: File Sharing
S: Finance Wireless
S: Finance and Investing
S: Food and Restaurants
S: Forums and Message Boards
S: Freeware and Shareware
S: Gambling
S: Gambling Wireless
S: Gaming
S: Glamour
S: Gore
S: Government
S: Hacking
S: Hate
```

```
S: Health
S: Hobbies
S: Hosting
S: Internet Telephony
S: Job Search
S: Kids
S: Law
S: Lifestyle
S: Mature Content
S: Military
S: Mobile Entertainment
S: Music
S: News
S: News Wireless
S: Non profit
S: Occult
S: Personal Ads and Dating
S: Personal Ads andd Dating Wireless
S: Pets
S: Placeholder
S: Politics
S: Pornography
S: Pornography Wireless
S: Portal
S: Proxy Wireless
S: Real Estate
S: Reference
S: Religion
S: Science
S: Search
S: Self Harm
S: Sexual Education
S: Shopping
S: Sports
S: Sports Wireless
S: Streaming Media
S: Suicide
S: Technology and Telecommunications
S: Tobacco
S: Travel
S: Travel Wireless
S: Violence
S: Virtual Community
```

```
S: Weapons
S: Webmail
S: Wedding
S: AllowURLsCategory
S: URLReputation
S: ;
S:
S: 0
S:
```

This response informs the client of the following:

- Besides the OPTIONS method, the only supported method is RESPMOD and FILEMOD.
- The optional 204 shortcut is supported.
- Four bytes of preview information are preferred.
- All files should be sent for preview.
- The data in this response can be cached up to one hour.
- The server supports a maximum of 128 simultaneous connections.
  The maximum number of simultaneous connections that Symantec Protection Engine supports varies on the operating environment.

Scanning HTTP requests (REQMOD)

The legacy service, AVSCANREQ, supports antivirus scanning only. The SYMCScanReq* services handle scanning for viruses and URL filtering. You can determine whether you want antivirus scanning only, URL filtering only, or antivirus and URL filtering scanning. SYMCScanReq-AV and SYMCScanReqEx-AV scans only for viruses on POST transactions. SYMCScanReq-AV-URL and SYMCScanReqEx-AV-URL scans for viruses on POST transactions and URL filtering on all transactions.

Symantec Protection Engine supports the following format for specifying scan, repair and block services:

```
icap://server.name:port/symcscanreq-av-url
```

where server.name is the name of the server on which Symantec Protection Engine is running. The port number is optional if Symantec Protection Engine is running on port 1344, which is the default ICAP port.

See “About ICAP responses” on page 25.

REQMOD examples

The ICAP client sends an HTTP request to Symantec Protection Engine, which then returns any of the following responses:

- An unmodified version of the original request
- An HTTP response indicating success or forbidden (for example, virus found or content blocked)
- Error condition (for example, bad gateway)

Examples of REQMOD services are as follows:

- REQMOD antivirus-scanning example
- REQMOD URL filtering scanning example
- REQMOD antivirus and URL filtering scanning example

REQMOD antivirus-scanning example

A sample REQMOD request on SYMCScanReq-AV is as follows:

```
C: REQMOD icap://172.16.11.19:1344/SYMCScanReq-AV ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, req-body=136
C:
C: POST frere.exe HTTP/1.1
C: Host:icheck.symantec.com
C: Accept: text/html, text/plain
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "DBDF573DB137CC3FD88B5C294F14427F"
S: Date: Mon Apr 23 06:59:43 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQ-AV
S: X-Violations-Found: 1
S:        frere.exe
S:        Jeru.1808.Frere Jac
```

```
S:        755
S:        0
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S:
S: HTTP/1.1 403 Forbidden.
S: Connection: close
S: Content-Length: 671
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 29f
S: Getting chunk of size 671 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section.

A sample REQMOD request on SYMCScanReqEx-AV is as follows:

```
C: REQMOD icap://127.0.0.1:1344/SYMCScanReqEx-AV ICAP/1.0
C: Host: 127.0.0.1:1344
C: Connection: close
C: Encapsulated: req-hdr=0, req-body=129
C:
C: post eicar.com HTTP/1.1
C: Host:icheck.symantec.com
C: Accept: text/html, text/plain
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "0A6D2000EC0B80EC89B89072963907C6"
S: Date: Wed Jul 25 11:50:30 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.44
S: Service-ID: SYMCSCANREQEX-AV
S: X-Violations-Found: 1
```

```
S:      eicar.com
S:      EICAR Test String| ViralThreat=Virus|
SubCategoryID=0| UberCategories=Malware|
CumulativeRiskRating=High| PerformanceImpact=High|
PrivacyImpact=High| EaseOfRemoval=High| Stealth=High|
SubCategoryDescription=Programs that infect other programs,
files, or areas of a computer by inserting thems
elves or attaching themselves to that medium.
S:      11101
S:      0
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S:
S: HTTP/1.1 403 Forbidden.
S: Connection: close
S: Content-Length: 257
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 101
S: Getting chunk of size 257 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section. In addition,the ICAP X-Violations-Found response header includes enhanced threat categorization information like threat category name (ViralThreat or NonViralThreat), SubCategoryID, UberCategories, CumulativeRiskRating, PerformanceImpact, PrivacyImpact, EaseOfRemoval, Stealth and SubCategoryDescription.

REQMOD URL filtering scanning example

A sample REQMOD request on SYMCScanReq-URL is as follows:

```
C: REQMOD icap://172.16.11.19:1344/SYMCSCANREQ-URL ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, null-body=130
C:
C: get / HTTP/1.1
C: Host: www.cnn.com
C: Accept: text/html, text/plain
```

```
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
S: ICAP/1.0 201 Created
S: ISTag: "A3EB96E4EB5FB056774EB9AF72CB41AC"
S: Date: Sat Apr 21 09:19:20 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQ-URL
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S: X-Attribute: Technology and Telecommunications
S: X-URL-Blocked-Domain: symantec.com
S:
S: HTTP/1.1 403 Forbidden.
S: Connection: close
S: Content-Length: 641
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 281
S: Getting chunk of size 641 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a block message response is returned because the requested URL was found in a URL category that was configured to be denied in the Symantec Protection Engine policies. In this example, the URL was found in the “Technology and Telecommunications” category.

A sample REQMOD request on SYMCScanReq-URL, if the URL belongs to the CAIC category, is as follows:

```
C: REQMOD icap://172.16.11.19:1344/SYMCScanReq-URL ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, null-body=114
C:
C: get / HTTP/1.1
C: Host:caic.test
C: Accept: text/html, text/plain
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
```

```
S: ICAP/1.0 201 Created
S: ISTag: "D0C2E01BD428B3C9AA10F0492C2D9373"
S: Date: Sun May 20 05:10:32 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQ-URL
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S: X-Attribute: CAIC
S: X-URL-Blocked-Domain: CAIC-URL
S:
S: HTTP/1.1 403 Forbidden.
S: Connection: close
S: Content-Length: 585
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 249
S: Getting chunk of size 585 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a block message response is returned because the requested URL was found in a URL category that was configured to be denied in the Symantec Protection Engine policies. In this example, the URL was found in the “CAIC” category.

REQMOD antivirus and URL filtering scanning example

A sample REQMOD request on SYMCScanReq-AV-URL is as follows:

```
C: REQMOD icap://172.16.11.19:1344/SYMCScanReq-AV-URL ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, req-body=147
C:
C: POST annacar-lzh-rar-hqx-exe.uue HTTP/1.1
C: Host:icheck.symantec.com
C: Accept: text/html, text/plain
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
C: 44
C: Sending chunk of size 68 bytes
```

```
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "C9893261C2EBC2F648DFC0FCCA87297D"
S: Date: Sat Apr 21 09:25:10 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQ-AV-URL
S: X-Violations-Found: 2
S:      annacar-lzh-rar-hqx-exe.uue/annacar-lzh-rar-hqx.exe
/annacar-lzh-rar.
        hqx/ANNACA~1.RAR/annacar.lzh/ANNAREP.COM
S:      Anna
S:      42
S:      0
S:      annacar-lzh-rar-hqx-exe.uue/annacar-lzh-rar-hqx.exe
/annacar-lzh-rar.
        hqx/ANNACA~1.RAR/annacar.lzh/EICAR.COM
S:      EICAR Test String
S:      11101
S:      0
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S: X-Attribute: TechnologyandTelecommunication
S: X-URL-Blocked-Domain: symantec.com
S:
S: HTTP/1.1 403 Forbidden.
S: Connection: close
S: Content-Length: 646
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 286
S: Getting chunk of size 646 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section. A block message response is returned because the requested URL was found in a URL category that was configured to be denied in the Symantec Protection Engine policies. In this example, the URL was found in the “Technology and Telecommunication” category.

A sample REQMOD request on SYMCScanReq-AV-URL, if the URL belongs to the CAIC category, is as follows:

```
C: REQMOD icap://172.16.11.19:1344/SYMCScanReq-AV-URL ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, req-body=147
C:
C: POST annacar-lzh-rar-hqx-exe.uue HTTP/1.1
C: Host:caic.test
C: Accept: text/html, text/plain
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
C: 160e2
C: Sending chunk of size 90338 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "7A6C504FEF0B1FA36A8B28967C08B108"
S: Date: Sun May 20 05:10:32 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQ-AV-URL
S: X-Violations-Found: 2
S:        annacar-lzh-rar-hqx-exe.uue/annacar-lzh-rar-hqx.exe
/annacar-lzh-rar.
        hqx/ANNACA~1.RAR/annacar.lzh/ANNAREP.COM
S:        Anna
S:        42
S:        0
S:        annacar-lzh-rar-hqx-exe.uue/annacar-lzh-rar-hqx.exe
/annacar-lzh-rar.
        hqx/ANNACA~1.RAR/annacar.lzh/EICAR.COM
S:        EICAR Test String
S:        11101
S:        0
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S: X-Attribute: CAIC
S: X-URL-Blocked-Domain: CAIC-URL
S:
S: HTTP/1.1 403 Forbidden.
```

```
S: Connection: close
S: Content-Length: 654
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 28e
S: Getting chunk of size 654 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section. A block message response is returned because the requested URL was found in a URL category that was configured to be denied in the Symantec Protection Engine policies. In this example, the URL was found in the “CAIC” category.

A sample REQMOD request on SYMCScanReqEx-AV-URL is as follows:

```
C: REQMOD icap://127.0.0.1:1344/SYMCScanReqEx-AV-URL ICAP/1.0
C: Host: 127.0.0.1:1344
C: Connection: close
C: Encapsulated: req-hdr=0, req-body=136
C:
C: post www.symantec.com HTTP/1.1
C: Host:icheck.symantec.com
C: Accept: text/html, text/plain
C: Accept-Encoding: compress
C: Pragma: no-cache
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "C9893261C2EBC2F648DFC0FCCA87297D"
S: Date: Sat Apr 21 09:25:21 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANREQEX-AV-URL
S: X-Violations-Found: 1
S: www.symantec.com
S: EICAR Test String| ViralThreat=Virus|
SubCategoryID=0| UberCategories=Malware|
CumulativeRiskRating=High| PerformanceImpact=High|
PrivacyImpact=High| EaseOfRemoval=High| Stealth=High|
SubCategoryDescription=Programs that infect other programs, files,
or areas of a computer by inserting
themselves or attaching themselves to that medium.
S: 11101
S: 0
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=110
S: X-Attribute: Technology and Telecommunications
S: X-URL-Blocked-Domain: symantec.com
S:
S: HTTP/1.1 403 Forbidden.
S: Connection: close
S: Content-Length: 646
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 286
S: Getting chunk of size 646 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section. In addition,the ICAP X-Violations-Found response header includes enhanced threat categorization information like threat category name (ViralThreat or NonViralThreat), SubCategoryID, UberCategories, CumulativeRiskRating, PerformanceImpact, PrivacyImpact, EaseOfRemoval, Stealth and SubCategoryDescription.

A block message response is returned because the requested URL was found in a URL category that was configured to be denied in the Symantec Protection Engine policies. In this example, the URL was found in the “Technology and Telecommunication” category.

Scanning HTTP responses (RESPMOD)

The legacy services, AVSCAN and AVSCANRESP, support antivirus scanning only. Even the SYMCScanResp* (SYMCScanResp-AV, SYMCScanResp-AV-DDR, SYMCScanRespEx-AV) services handle scanning for viruses only.

Symantec Protection Engine supports the following format for specifying scan, repair and block services:

```
icap://server.name:port/symcscanresp-av-ddr
```

where server.name is the name of the server on which Symantec Protection Engine is running. The port number is optional if Symantec Protection Engine is running on port 1344, which is the default ICAP port.

See “About ICAP responses” on page 25.

RESPMOD examples

The ICAP client sends an HTTP response (including the HTTP request headers) to Symantec Protection Engine, which then returns any of the following responses:

- An unmodified version of the original response
- A modified response, indicating what was found
- Error condition (for example, bad gateway)

Examples of RESPMOD services are as follows:

- RESPMOD antivirus-scanning example
- RESPMOD antivirus and URL filtering scanning example

RESPMOD antivirus-scanning example

A sample RESPMOD on SYMCScanResp-AV response is as follows:

```
C: RESPMOD icap://172.16.11.19:1344/SYMCSCANRESP-AV ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=52, res-body=71
C:
C: get / HTTP/1.1
C: Host:icheck.symantec.com
C:
C: HTTP/1.1 200 OK
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "DBDF573DB137CC3FD88B5C294F14427F"
S: Date: Sat Apr 21 07:40:36 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
```

```
S: Service-ID: SYMCSCANRESP-AV
S: X-Violations-Found: 1
S:      index.html/frere.exe
S:      Jeru.1808.Frere Jac
S:      755
S:      2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=83
S:
S: HTTP/1.1 200 OK
S: Content-Length: 671
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 29f
S: Getting chunk of size 671 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section.

A sample RESPMOD on SYMCScanRespEx-AV response is as follows:

```
C: RESPMOD icap://127.0.0.1:1344/SYMCScanRespEx-AV ICAP/1.0
C: Host: 127.0.0.1:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=52, res-body=71
C:
C: get eicar.com HTTP/1.1
C: Host:icheck.symantec.com
C:
C: HTTP/1.1 200 OK
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "44C5020856436B4C8FF7F8EA9F287653"
S: Date: Tue Jul 24 18:13:43 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.44
```

```
S: Service-ID: SYMCSCANRESPEX-AV
S: X-Violations-Found: 1
S: eicar.com
S: EICAR Test String| ViralThreat=Virus| SubCategoryID=0|
UberCategories=Malware| CumulativeRis
kRating=High| PerformanceImpact=High| PrivacyImpact=High|
EaseOfRemoval=High| Stealth=High| SubCategoryDescription=Programs
that infect other programs, files, or areas of a computer by inserting
themselves or attaching themselves to that medium.
S: 11101
S: 2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=83
S:
S: HTTP/1.1 200 OK
S: Content-Length: 257
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 101
S: Getting chunk of size 257 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section. In addition,the ICAP X-Violations-Found response header includes enhanced threat categorization information like threat category name (ViralThreat or NonViralThreat), SubCategoryID, UberCategories, CumulativeRiskRating, PerformanceImpact, PrivacyImpact, EaseOfRemoval, Stealth and SubCategoryDescription.

RESPMOD URL filtering scanning example

A sample RESPMOD on SYMCScanResp-DDR response is as follows:

```
C: RESPMOD icap://172.16.11.19:1344/SYMCSCANRESP-DDR ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=44, res-body=63
C:
C: get / HTTP/1.1
C: Host:icheck.symantec.com
C:
```

```
C: HTTP/1.1 200 OK
C:
C: 3ef7
C: Sending chunk of size 16119 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "7E823734E7070EECD74143AF7CCA7447"
S: Date: Sun May 20 05:10:32 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-DDR
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=83
S: X-Attribute: Sex/Acts
S:
S: HTTP/1.1 200 OK
S: Content-Length: 559
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 22f
S: Getting chunk of size 559 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a block message response is returned because the threshold was exceeded for a content category that was configured to be denied in the Symantec Protection Engine policies. This example returns a block message response because the threshold exceeded the value that was set for the Sex/Acts category.

RESPMOD antivirus and URL filtering scanning example

A sample RESPMOD on SYMCScanResp-AV-DDR response is as follows:

```
C: RESPMOD icap://172.16.11.19:1344/SYMCScanResp-AV-DDR ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=52, res-body=71
C:
C: get eicar.com HTTP/1.1
C: Host:icheck.symantec.com
```

```
C:
C: HTTP/1.1 200 OK
C:
C: 44
C: Sending chunk of size 68 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "DBDF573DB137CC3FD88B5C294F14427F"
S: Date: Mon Apr 23 08:00:46 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-AV-DDR
S: X-Violations-Found: 1
S:      eicar.com
S:      EICAR Test String
S:      11101
S:      2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: res-hdr=0, res-body=83
S:
S: HTTP/1.1 200 OK
S: Content-Length: 671
S: Pragma: no-cache
S: Content-Type: text/html
S:
S: 29f
S: Getting chunk of size 671 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section.

As the DDR service has been deprecated from SSE 5.2.10, no content filtering is done on the request. The response is returned as 200 OK in this case.

Scanning non-HTTP data (RESPMOD and FILEMOD)

Not all Symantec Protection Engine clients process HTTP data. Network attached storage devices handle files. Mail transfer agents handle email messages. The files to be scanned can either be sent to Symantec Protection Engine over the network connection or accessed on the file system of the computer that is running Symantec Protection Engine.

See “Scanning HTTP responses (RESPMOD)” on page 66.

See “Local file scanning (FILEMOD)” on page 73.

About network scanning (RESPMOD)

Network scanning is accomplished by mimicking an HTTP response scan. An ICAP request is created that includes manufactured HTTP requests and response headers. The file to be scanned is included as the HTTP message. The HTTP request headers must include a request line with the file name. Typically, the HTTP GET method is used. The HTTP response headers can be the HTTP 200 OK response line.

See “Scanning HTTP responses (RESPMOD)” on page 66.

See “About ICAP responses” on page 25.

Network scanning example

An example of a RESPMOD request is as follows:

```
C: RESPMOD icap://172.16.11.19:1344/SYMCScanResp-AV-DDR ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=63, res-body=82
C:
C: get E_Games_Gerganna.txt HTTP/1.1
C: Host:icheck.symantec.com
C:
C: HTTP/1.1 200 OK
C:
C: 4670
C: Sending chunk of size 18032 bytes
C:
C: 0
C:
S: ICAP/1.0 201 Created
S: ISTag: "E15593F868A67774FAE09EE52232DA93"
S: Date: Date: Sun May 20 05:10:32 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-AV-DDR
S: X-Violations-Found: 2
S:       E_Games_Gerganna.txt/annarep.com
S:       Anna
```

```
S:         42
S:         1
S:         E_Games_Gerganna.txt/gergana.exe
S:         Gergana.182
S:         550
S:         2
S: X-Outer-Container-Is-Mime: 1
S: Encapsulated: res-hdr=0, res-body=57
S:
S: HTTP/1.1 200 OK
S: Via: 1.1 Symantec Protection Engine (ICAP)
S:
S: 430a
S: Getting chunk of size 17162 bytes
S:
S: 0
S:
```

This response returns a 201 Created status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section.

Local file scanning (FILEMOD)

In the file modification (FILEMOD) mode, an ICAP client sends an ICAP request that contains a file location (with the full path specified) to an ICAP server.

The ICAP server might then do any of the following:

- Send back an ICAP response that contains only headers and no body
- Return an error

This response will contain information about the modification that was performed on the file in-place.

Local file scanning is accomplished by sending an ICAP request with a FILEMOD method to any of the services that handle the FILEMOD method. A Symantec ICAP extension header X-Filepath contains the full path to the file from the point-of-view of the server. If the server cannot access a file at the specified location, a 502 Bad Gateway response is sent. If no X-Filepath header is received, a 400 Bad Request response is sent. The response will be similar to a RESPMOD request for the same file but will contain no HTTP headers and a null-body.

See “About ICAP responses” on page 25.

FILEMOD examples

Examples of RESPMOD services are as follows:

- FILEMOD antivirus-scanning example
- FILEMOD antivirus and URL filtering scanning example

FILEMOD antivirus-scanning example

A sample FILEMOD response on SYMCScanResp-AV is as follows:

```
C: FILEMOD icap://172.16.11.19:1344/SYMCScanResp-AV ICAP/1.0
C: Host: 172.16.11.19:1344
C: X-Filepath: d:\vfiles\test2\frere.exe
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 403 Forbidden.
S: ISTag: "CC0209F0E11B8594E4BC3043E014D818"
S: Date: Sun May 20 05:10:32 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-AV
S: X-Violations-Found: 1
S:       frere.exe
S:       Jeru.1808.Frere Jac
S:       755
S:       2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: null-body=0
S:
```

This response returns a 403 Forbidden status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section.

A sample FILEMOD response on SYMCScanRespEx-AV is as follows:

```
C: FILEMOD icap://127.0.0.1:1344/SYMCScanRespEx-AV ICAP/1.0
C: Host: 127.0.0.1:1344
C: X-Filepath: d:\SDK-Automation\input-testdata\eicar.com
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 403 Forbidden.
S: ISTag: "44C5020856436B4C8FF7F8EA9F287653"
S: Date: Tue Jul 24 18:13:59 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.44
```

```
S: Service-ID: SYMCSCANRESPEX-AV
S: X-Violations-Found: 1
S: eicar.com
S: EICAR Test String| ViralThreat=Virus| SubCategoryID=0|
UberCategories=Malware| CumulativeRiskRating=High|
PerformanceImpact=High| PrivacyImpact=High|
EaseOfRemoval=High| Stealth=High| SubCategoryDescription=Programs
that infect other programs, files, or areas of a computer by inserting
themselves or attaching themselves to that medium.
S: 11101
S: 2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: null-body=0
S:
```

This response returns a 403 Forbidden status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section. In addition,the ICAP X-Violations-Found response header includes enhanced threat categorization information like threat category name (ViralThreat or NonViralThreat), SubCategoryID, UberCategories, CumulativeRiskRating, PerformanceImpact, PrivacyImpact, EaseOfRemoval, Stealth and SubCategoryDescription.

FILEMOD URL filtering scanning example

A sample FILEMOD response on SYMCScanResp-DDR is as follows:

```
C: RESPMOD icap://172.16.11.19:1344/SYMCScanResp-DDR ICAP/1.0
C: Host: 172.16.11.19:1344
C: Connection: close
C: Encapsulated: req-hdr=0, res-hdr=63, res-body=82
C:
C: get E_Games_Gerganna.txt HTTP/1.1
C: Host:icheck.symantec.com
C:
C: HTTP/1.1 200 OK
C:
C: 4670
C: Sending chunk of size 18032 bytes
C:
C: 0
C:
S: ICAP/1.0 200 OK
S: ISTag: "27FAA105B2F0F2EC9F7F359A081AE1FF"
S: Date: Sun May 20 05:10:32 2012 GMT
```

```
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-DDR
S: X-Outer-Container-Is-Mime: 1
S: Encapsulated: res-hdr=0, res-body=57
S:
S: HTTP/1.1 200 OK
S: Via: 1.1 Symantec Protection Engine (ICAP)
S:
S: 4670
S: Getting chunk of size 18032 bytes
S:
S: 0
S:
```

This response returns a 403 Forbidden status, which indicates that a problem was found. In this example, a block message response is returned because the threshold was exceeded for a URL category that was configured to be denied in the Symantec Protection Engine policies. This example, the threshold exceeded the value that was set for the Sex/Acts category.

FILEMOD antivirus and URL filtering scanning example

A sample FILEMOD response on SYMCScanResp-AV-DDR is as follows:

```
C: FILEMOD icap://172.16.11.19:1344/SYMCScanResp-AV-DDR ICAP/1.0
C: Host: 172.16.11.19:1344
C: X-Filepath: C:\Viruses\eicar.com
C: Connection: close
C: Encapsulated: null-body=0
C:
S: ICAP/1.0 403 Forbidden.
S: ISTag: "592477508F2C4951E283649329C89CD2"
S: Date: Sun May 20 05:10:32 2012 GMT
S: Service: Symantec Protection Engine/7.0.0.31
S: Service-ID: SYMCSCANRESP-AV-DDR
S: X-Violations-Found: 1
S:       eicar.com
S:       EICAR Test String
S:       11101
S:       2
S: X-Outer-Container-Is-Mime: 0
S: Encapsulated: null-body=0
S:
```

This response returns a 403 Forbidden status, which indicates that a problem was found. In this example, a virus was found, which is indicated in the X-Violations-Found section.

As the DDR service has been deprecated from SSE 5.2.10, no content filtering is done on the request. The response is returned as 200 OK in this case.

Index