



Symantec™ Threat Isolation Platform Guide for Administrators

Version 1.13

September 2019



Guide for Administrators - Revisions

Version	Date	New/Enhanced Features
1.13	September 2019	<ul style="list-style-type: none">■ Bandwidth Usage Reduction■ Browser's Native Menu Support■ Data Criteria Matching in Request Body■ Data Leakage Prevention Server Settings integrated in Upload Profile Scan Settings■ Document Isolation Actions Policy■ Exporting Activity Logs Analytics and Narrow By Filter Results to PDF■ Gateway Cluster Time Zone Selection■ Geolocation Destination Match Criteria■ Isolation Policy for iframes■ Inspect Advanced Settings in Download and Upload Profiles■ Isolation Indication Custom Color■ Keytab Settings Workflow Modifications■ Management Users "Terms of Use" Page■ Media Quality - Controlling Audio, Video and Image Settings■ Mobile Browser Rendering Support■ Multiple Organizations■ Native Context Menu Support■ Prompting End User Before File Download■ Request Filters Data Criteria■ Rule Editing New Capabilities■ SAML Authentication in Management Users■ Session Activity Settings■ Symantec Cynic Sandbox■ Website Subresources Policy in Rule Advanced Settings



Version	Date	New/Enhanced Features
1.12	December 2018	<ul style="list-style-type: none">■ Authentication Connectivity Improvements■ Block Page Integration■ Clear Authorization Claims■ Cloning Objects■ Convenient Activation of Report Server■ Customized List of URLs in VRM for Grid Rendering■ Doc Isolation Viewer: Open File in New Tab■ Email Threat Isolation (ESS/SMG)■ Enhanced Granularity for Download Scanner Settings■ Media Quality■ Read-Only Enhancements■ Symantec AV Support■ Votiro v3.0 Support
1.11	September 2018	<ul style="list-style-type: none">■ Anti-Bot Protection■ Customized Text for Untrusted Certificate Message■ Gateway Audit Logs■ Management Identity Providers■ Management Roles■ On-premises Document Isolation Server■ SNMP Servers■ Trusting Only Imported Certificates
1.10	April 2018	<ul style="list-style-type: none">■ Application Destination■ Downstream Proxy■ Easy Gateway Registration■ Licensing■ Log Forwarding to Apache Kafka■ Next Hop Proxy/Server■ Risk Levels
1.9	December 2017	<ul style="list-style-type: none">■ About Symantec Threat Isolation Dialog■ License Agreement■ New Gateway/PDP Registration■ Private Data Processing■ SAML IdP Configuration Web■ Troubleshooting■ Web Application Isolation Mode
1.8	July 2017	<ul style="list-style-type: none">■ ArcSight CEF Fields Mapping■ Management Supported Browsers■ Minimum System Requirements■ Read-Only Webpages



Contents

1	Preface	19
1.1	Abstract	19
1.2	Document Purpose	20
1.3	Using this Document	20
1.4	References	21
1.5	Terminology	21
2	Symantec Threat Isolation Solution Overview	23
2.1	Goals and Scenarios	23
2.2	Returned HTML Content	24
2.3	High-level Data Architecture	24
	Data Flow	25
2.4	Platform Components	26
2.5	Protection Scenarios	27
2.5.1	Overview	27
2.5.2	Protecting an Organization's Endpoints from Attack	28
2.5.3	Protecting an Organization's Web Applications from Attack	30
2.6	Deployment Topologies	30
2.6.1	Overview	30
2.6.2	Symantec Threat Isolation Explicit Proxy	31
2.6.3	Symantec Threat Isolation with Downstream Proxy Forwarding	32
2.6.4	Symantec Threat Isolation with Block Page Integration	32
2.6.5	Symantec Email Threat Isolation	34
2.6.6	Symantec Threat Isolation as Web Application Isolation Gateway Mode	37
2.6.6.1	Using a Load Balancer	37
2.6.6.2	Not Using a Load Balancer	38



2.7	Cloud Services	39
2.8	How Symantec Threat Isolation Processes Private Data	39
2.8.1	Cookies and Session Data	40
2.8.2	Browsing Logging Data	40
2.8.3	Cloud Telemetry Data	41
2.8.4	Third-Party File Sanitizer Data	41
2.8.5	Document Viewer Data	42
2.8.6	Flash Activation Request Data	42
2.9	Reducing Bandwidth Usage	42
3	Installing the Symantec Threat Isolation Platform	43
3.1	System Requirements	43
3.2	Supported Platforms	44
3.3	Supported Browsers	45
3.3.1	Management Browser	45
3.3.2	Endpoint Browser	45
3.4	Preparing for Symantec Threat Isolation Platform Installation ..	46
3.4.1	Overview	46
3.4.2	Defining Components Per Machine	46
3.4.3	Defining Networking	48
3.4.3.1	TIE Public DNS Name Considerations	49
3.4.4	Signing the CA Certificate	50
3.4.4.1	Prerequisite	52
3.4.4.2	Generating the Encrypted Private Key	52
3.4.4.3	Signing the CA Certificate File	54
3.4.4.4	Transferring Encrypted Private Key and CA Certificate File ...	56
3.5	Installing the Symantec Threat Isolation Platform	56
3.5.1	Overview	56
3.5.2	Preparing the Symantec Threat Isolation Platform Machine	58



3.5.3	Downloading the ISO File and Verifying the MD5 Signature .	58
3.5.4	Configuring the Machine for Loading the ISO File	59
3.5.5	Booting the Machine and Starting Installation	59
3.5.5.1	Changing the Operating System Password	61
3.5.6	Initializing the Symantec Threat Isolation Platform	61
3.5.6.1	Initializing the Symantec Threat Isolation Platform	61
3.5.6.2	Initializing the Management Gateway	61
3.5.7	Defining the Management Gateway	62
3.5.8	Defining Symantec Threat Isolation Components	71
3.5.8.1	Deciding Where the PDP Will Reside	72
3.5.9	Initializing Gateways	73
	Registering the Gateway	74
3.5.9.1	Checking Gateway Registrations	76
3.5.10	Associating the CA Certificate with Your Zone	76
3.5.11	Installing the CA Certificate as Trusted Root CA on the Client Side	77
3.5.11.1	Deploying the CA Certificate File to the End Users	77
3.5.11.2	Installing the CA Certificate in Windows Browsers	78
3.5.11.3	Installing the CA Certificate in a Firefox Browser	82
3.5.11.4	Installing the CA Certificate on a Mac Machine	82
3.5.12	Verifying the Trusted Root CA in the Endpoint Browser ...	84
3.5.13	Making Sure Third-Party Cookies Are Accepted	84
3.6	Configuring Your Deployment Topology	86
3.6.1	Configuring the Symantec Threat Isolation Explicit Proxy Topology	87
3.6.1.1	Editing the Proxy Auto-Configuration (PAC) File	87
3.6.1.2	Configuring the PAC File in a Single Endpoint Browser	87
		90
3.6.1.3	Verifying PAC File Configuration in the Endpoint Browser	90



3.6.1.4	Defining Firewall Rules	94
3.6.2	Configuring Symantec Threat Isolation with Downstream Proxy Forwarding	98
3.6.2.1	Configuring the Downstream Proxy for Communication over HTTPS	101
	Adding forwarding hosts to the downstream proxy	101
	SSL Inspection	101
	Adding rules to the downstream proxy for HTTPS	101
3.6.2.2	Configuring the Downstream Proxy for Communication over HTTP	101
	Adding rules to the downstream proxy for HTTP	101
3.6.2.3	Defining Firewall Rules	102
3.6.3	Configuring Symantec Threat Isolation with Block Page Integration	105
3.6.3.1	Configuring the NGFW/SWG to Redirect Traffic to the Isolation Portal	105
3.6.3.2	Placing a Transparent SWG between NGFW and Threat Isolation	106
3.6.3.3	Defining Firewall Rules	106
3.6.4	Configuring Symantec Email Threat Isolation	109
3.6.4.1	Defining Firewall Rules	109
3.6.5	Configuring Symantec Threat Isolation as Web Application Isolation Gateway Mode	112
3.6.5.1	Defining Firewall Rules	112
3.6.6	Pushing Settings to the Gateways	114
3.7	Viewing Version and License Information, Credits	114
3.8	Moving Management to a Different Server	114
3.9	Upgrading the Symantec Threat Isolation System	114
3.9.1	Upgrading from Version 1.10 to Version 1.13	115
3.9.2	Upgrading from Version 1.11 to Version 1.13	115



3.10	Performing Shutdown	115
3.11	Performing Backup, Restore and Reset Procedures	116
3.11.1	Backing Up System Data	116
3.11.2	Restoring System Data	116
3.11.3	Resetting a Management User Password	117
3.11.3.1	Password Policy	117
3.11.4	Restoring the Default Settings	118
4	Configuring Security Policy Settings	119
4.1	Overview	119
4.2	Defining Security Policies and Rules	120
4.2.1	Menu Search	120
4.2.2	Editing Your Policy	120
4.2.2.1	Defining Authentication Profiles	124
4.2.2.2	Authentication Mode	124
	Proxy Authentication Mode	125
	Server Authentication Mode	126
4.2.2.3	Authentication Caching	128
4.2.2.4	System Rules	129
4.2.3	Source Application Policy Rules	129
4.2.4	Working with Policies	130
4.2.5	Enforcing Policies	131
4.2.6	Match Criteria Flow	131
4.2.7	Defining Policy Rules	132
4.2.7.1	Source Geolocations	137
4.2.7.2	Rule Actions	137
	Limited Inspect Action	141
	Selective Isolation in Online Service Suites	141
4.3	Defining Profiles	142



4.3.1	Accessing Profiles	143
4.3.2	Cloning Objects	143
4.3.3	Defining Isolation Profiles	143
4.3.3.1	Overview	143
4.3.3.2	Adding an Isolation Profile	144
4.3.4	Defining Download Profiles	149
4.3.4.1	Overview	149
Download Profile Actions	149	
4.3.4.2	Document Isolation Viewer	151
Using an On-Premises Document Isolation Server	151	
Opening Documents in New Tab in Document Isolation Viewer	152	
4.3.4.3	Downloading Files Safely	152
Symantec AV (Anti-Virus)	153	
4.3.4.4	Adding a Download Profile	153
4.3.4.5	Defining Download Profiles Advanced Settings	158
Configuring File Sanitizer Settings per Download Profile	158	
Configuring Symantec Cynic Scanning Mode for a Download Profile	158	
Opening Documents in New Tab in Document Isolation Viewer	158	
Prompting the End User Before File Download	159	
4.3.5	Defining Upload Profiles	159
4.3.5.1	Overview	159
4.3.5.2	Adding an Upload Profile	160
4.3.6	Defining Activity Log Profiles	163
4.3.6.1	Overview	163
4.3.6.2	Adding an Activity Log Profile	163
4.3.6.3	URL Query Parameter Privacy	165
4.3.7	Defining End-User Data Protection Profiles	166
4.3.7.1	Overview	166



4.3.7.2	Adding an End-User Data Protection Profile	166
4.3.8	Defining Application Data Protection Profiles	167
4.3.8.1	Overview	167
4.3.8.2	Adding an Application Data Protection Profile	167
4.3.8.3	Opening Developer Tools Remotely	168
4.3.9	Defining Anti-Bot Protection Profiles	170
4.3.9.1	Overview	170
4.3.9.2	Adding an Anti-Bot Protection Profile	170
4.3.9.3	Customizing the Anti-Bot Captive Page	171
4.4	Defining Policy Entities	173
4.4.1	Accessing Policy Entities	173
4.4.2	Managing Threat Isolation in Multiple Organizations	173
4.4.2.1	Creating Organizations	173
4.4.3	Creating Access Roles	174
4.4.4	Categorizing Websites	176
4.4.4.1	Defining URL Categories	176
4.4.4.2	Defining Risk Levels	177
4.4.5	Controlling Non-Browser Application Objects	178
4.4.6	Creating Custom Pages	183
4.4.6.1	Creating a Custom Block Page	183
4.4.6.2	Creating a Custom Read-Only Page	185
4.4.7	Creating Network Objects and Object Groups	186
4.4.7.1	Defining Network Objects	186
4.4.7.2	Defining Network Object Groups	186
4.4.8	Creating URL Objects and Object Groups	187
4.4.8.1	Creating URL Objects	187
4.4.8.2	Creating URL Object Groups	187
4.4.9	Creating Request Filters	188



4.4.9.1	Creating a Request Filter	188
4.4.9.2	Creating Header Criteria	189
4.4.9.3	Creating Data Criteria	190
4.4.10	Creating Rule Advanced Settings	190
4.4.10.1	Enabling the End User to Temporarily Suspend Isolation	192
4.4.10.2	Idle Mode Setting	193
4.4.11	Creating Policy Advanced Settings	194
4.4.12	Creating Geolocation Objects	194
4.5	Defining Internal Users	195
4.5.1	Creating Internal Users and User Groups	195
4.5.1.1	Creating Internal Users	195
4.5.1.2	Creating Internal User Groups	196
4.5.2	Defining Active Directory Settings	196
4.5.3	Creating Keytab Settings	197
4.5.3.1	Keytab Requirements	198
4.5.4	Defining SAML Trust	199
	Creating a SAML Trust object	200
4.5.4.1	Defining SAML Trust for Microsoft AD FS	201
4.5.4.2	Defining SAML Trust for Generic SAML Identity Providers	203
4.5.4.3	Identity Provider (IdP) Requirements	209
4.5.4.4	Connectivity between Client and Identity Provider (IdP)	209
4.5.5	Defining SAML Identity Providers	210
4.5.5.1	LDAP Access Role	211
4.6	Defining Management Users	212
4.6.1	Creating Management Users	212
4.6.1.1	Configuring a Terms of Use Page for Management Users	213
4.6.2	Identity Providers	214
4.6.2.1	Creating RADIUS Identity Providers	214



4.6.2.2	Creating SAML Identity Providers	215
4.6.3	Management Roles	217
4.6.3.1	Assigning Members to Management Roles	218
4.6.4	Viewing Management Audit Logs	220
4.7	Defining Zones, Gateways, and Associated Components	222
4.7.1	System Security Policy Distribution Hierarchy	222
4.7.2	Configuring the Zone	223
4.7.2.1	Overview	223
4.7.2.2	Defining the Zone	223
4.7.2.3	Updating Threat Isolation Engine Affinity	224
4.7.2.4	Updating a Zone's PAC File	226
4.7.3	Understanding the Threat Isolation Gateway and Its Components	230
4.7.4	Selecting the Policy Distribution Point (PDP)	230
4.7.5	Understanding the Gateway Settings Table	231
4.7.6	Pushing Settings	232
4.7.7	Defining a Threat Isolation Gateway	234
4.7.7.1	Configuring a Next Hop Proxy/Server	240
4.7.7.2	Enabling Web Application Isolation Gateway Mode with a Load Balancer	240
	Configuring the Public DNS Name	241
	Adding a Server Certificate	241
	Configuring a Load Balancer Health Check	242
	Authentication	242
	Link Isolation URL	242
	Client Side Setup	243
4.7.8	Defining Gateway Advanced Settings	243
4.7.8.1	Enabling Web Application Isolation Gateway Mode - No Load Balancer	245



Adding a Server Certificate	245
Authentication	247
Link Isolation URL	247
Client Side Setup	247
4.7.8.2 Portal Isolation Mode	247
4.7.9 Defining Threat Isolation Engines (TIEs)	248
4.7.10 Defining Threat Isolation Proxies	248
4.7.11 Defining a Web Application Isolation Gateway	249
4.7.12 Defining Gateway Clusters	249
4.7.12.1 Overview	249
4.7.12.2 Defining a Gateway Cluster	250
4.7.13 Viewing Gateway Audit Logs	250
4.7.14 Integrating with Active Directory	252
4.8 Configuring System Certificates	252
4.8.1 System CA Certificates	252
4.8.2 System Server Certificates	253
4.8.3 Adding a System Certificate	253
4.9 Configuring Trusted Certificates	254
4.9.1 Trusted CA Certificates	254
4.9.2 Trusted Server Certificates	255
4.9.3 Adding a Trusted Certificate	256
4.9.4 Trusting Only Imported Certificates	257
4.9.5 Adding Customized Text to the Untrusted Certificate Message	257
4.10 Integrating a Downstream Proxy	257
4.10.1 Creating New Downstream Proxy Settings	258
4.10.1.1 Isolation Criteria	262
4.10.2 Configuring the Symantec Secure Web Gateway (ProxySG)	263



4.11	Creating New Next Hop Proxy/Server Settings	264
4.11.1	X-Forwarded-For (XFF) Request Header	266
4.11.2	X-Authenticated-User (XAU) Request Header	266
4.12	Configuring Email Servers	266
4.13	Configuring SNMP Servers	267
4.14	Configuring Syslog Servers	269
4.15	Configuring ArcSight Servers	270
4.15.1	AWS S3 Protocol Configuration	271
4.15.2	ArcSight CEF Mapping	272
4.15.2.1	Sample CEF Content	279
4.16	Configuring Apache Kafka Servers	279
4.17	Configuring Cynic Server Settings	281
4.18	Configuring Data Leakage Prevention Server Settings	282
4.18.1	Adding Data Leakage Prevention Server Settings	282
4.19	Editing Advanced Configuration	283
4.20	Licensing	284
4.20.1	Registering your Licensed Components	284
4.20.1.1	Prerequisites	284
4.20.1.2	Registration	284
4.20.1.3	Viewing Current License Information	286
4.20.1.4	Updating a License	286
4.20.2	Activating Add-ons	287
5	High Availability and Load Balancing	287
5.1	Overview	287
5.2	High Availability and Load Balancing Process	288
5.2.1	Proxy Auto-Configuration (PAC) File	288
5.2.1.1	PAC File with DNS	288
5.2.1.2	PAC File with External Load Balancing Software	288



5.2.2	Proxy	289
5.2.3	Threat Isolation Engine (TIE)	289
5.2.3.1	TIE Key Mechanisms	289
5.2.3.2	TIE Server List	290
5.2.3.3	Blacklist	290
5.2.3.4	Failover	290
5.2.3.5	Stickiness	290
6	Reports	291
6.1	Activity Logs and Analytics	291
6.1.1	Understanding the Activity Logs Window	291
6.1.2	Understanding the Logs Tab	294
6.1.2.1	Activity Logs Table Views	294
6.1.2.2	Activity Log Event Window	297
6.1.3	Understanding the Analytics Tab	298
	Widget Display Types	300
	Filtering by Analytics Categories	300
6.2	Filtering and Searching Logged Data	302
6.2.1	Filtering Using the Search Bar	302
6.2.2	Filtering Using the Time Field	302
6.2.3	Filtering Using the Narrow By Area	303
6.2.4	Filtering Using the Follow Session Option	303
6.2.5	Filtering by Displaying or Hiding Specific Columns	303
6.2.6	Filtering Using the Advanced Settings	304
6.2.7	Exporting Logged Data to CSV	305
6.2.8	Exporting Logged Data to PDF	306
6.3	Defining a Report Server	307
6.4	Log Forwarding	307
6.4.1	Configuring Log Forwarding	307



7	Monitoring	308
7.1	Event Logs	308
7.2	Monitor Groups	309
7.3	Metric Thresholds	310
8	User Experience	317
8.1	Context Menu Display	317
8.1.1	Custom Symantec Context Menu	317
8.1.2	Remote Developer Tools	317
8.1.3	Suspend Isolation	318
8.1.4	Render Adobe Flash	319
8.1.5	Send Feedback	319
8.1.6	Cut, Copy and Paste	321
8.1.6.1	Paste Functionality	321
8.1.7	Copy Image	321
8.2	File Download	322
8.2.1	Download Profiles	322
8.2.1.1	Profile Setting: Allow	322
8.2.1.2	Profile Setting: Block	323
8.2.1.3	Profile Setting: Scan	323
8.2.1.4	Profile Setting: View	323
8.3	File Upload	324
8.4	Data Leakage Prevention	325
8.5	Data Protection	326
8.6	Block Page	326
8.7	High Availability Failover	327
8.8	Pause Functionality	327
8.9	Read-Only Webpages	328
8.10	Ad Blocker	328



8.11	Untrusted Certificate	329
8.12	Anti-Bot Captive Page	330
8.13	Document Isolation Viewer: Linked File Opens in Same Tab ..	331
9	Troubleshooting	332
9.1	Tools	332
9.1.1	Activity Logs	332
9.1.2	FGDiag	332
9.1.2.1	Table of Common Connectivity Issues	334
9.1.3	fgcli	337
9.1.3.1	Diagnostic Commands	337
9.1.3.2	Statistics Commands	337
9.1.3.3	Miscellaneous fgcli Commands	338
9.2	Error Message Format	338
9.3	Common Issues	340
9.3.1	Client Side	340
9.3.1.1	CA Certificate Not Trusted	340
9.3.1.2	Internet Explorer Does Not Show Isolated Page; Chrome Does	341
9.3.1.3	Access to Any Isolated Webpage Is Blocked	342
9.3.1.4	Downloading A Bigger File Than Permitted by Policy	343
9.3.1.5	Flash Video Not Displayed	344
9.3.1.6	Paste Nonfunctional from the Custom Symantec Context Menu	345
9.3.1.7	Isolated Websites Look Different Than Non-Isolated Ones	345
9.3.1.8	SSL/TLS Secure Connection Error	346
9.3.1.9	Incorrect URL Categorization	347
9.3.1.10	Slowness Issues	348
9.3.1.11	Proxy.PAC File Not Accessible	348
9.3.1.12	Ad Blocker Detected	349



9.3.2	Management Side	350
9.3.2.1	Active Directory Settings Server Error	350
9.3.2.2	Push Settings	350
9.3.2.3	Licensing	351
	Online Registration Failure	351
	Online Update Failure	351
	Rule Warning	352
	Categorization Failure	352
9.3.3	Threat Isolation Gateway Side	353
9.3.3.1	Upgrade Failure	353
9.3.4	Unauthenticated Users in Activity Logs	354
9.3.4.1	Cannot Find Activity Log Assigned to Specific User	354
9.3.4.2	All Activity Logs Have “Unauthenticated” Users	354
9.3.4.3	Activity Log Displays “Generic User”	355



1 Preface

1.1 Abstract

Information security issues result not from lack of diligence, skill, priority, or investment. Rather, they come from the common element of most cybersecurity solutions: detection. A host of different solutions ultimately rely on detection, including so-called prevention solutions such as antivirus/anti-malware, network sandboxes, next-generation firewalls, web application firewalls, and so on. Detection creates an unsustainable arms race with attacks that render security ineffective, costly, and intolerably complex.

The Symantec Threat Isolation solution addresses this security weakness.

Symantec Threat Isolation assumes all web content and activities are risky, and acts as an air gap between users and web applications to completely eliminate threats. Symantec Threat Isolation is a client-less network security platform that uses a new model for security based on the concept of isolation.

Isolation creates a secure execution environment placed between users and the web where all potentially malicious content is executed and only a safe visual stream is sent to the user.

Because all content is executed away from the users, they are completely protected from malicious websites, emails, and documents; web applications remain safe from attacks by malicious or compromised users.

Instead of relying on malware detection, Symantec Threat Isolation protects organizations' end users from cyberattacks by isolating malware and preventing it from reaching endpoint browsers. Symantec Threat Isolation rule-based security policies allow only webpages that are isolated to reach endpoint browsers as visual elements or a visual stream. The webpage code never reaches the endpoint browser, and therefore never runs in the browser.

Symantec Threat Isolation protects organizations' applications by isolating them. Isolation prevents the sending of HTTP requests directly to web applications, since only user gestures can be sent from the browser. This way, an end user cannot exploit the application data by running SQL injection attacks.

Policy rules control end user actions such as copy, paste, and so on, thus preventing data leakage from the application.



1.2 Document Purpose

This Guide for Administrators provides the Symantec Threat Isolation system administrator with instructions for deploying, integrating, configuring and managing the Symantec Threat Isolation system installed on the organization's site or as a cloud service. This guide also discusses day-to-day operation, system data logging and analytics, and system health.

1.3 Using this Document

This document includes the following chapters:

- Chapter [2, Symantec Threat Isolation Solution Overview](#) – Provides an overview of the Symantec Threat Isolation system, its usage scenarios, and other information needed for a basic understanding of the system.
- Chapter [3, Installing the Symantec Threat Isolation Platform](#) – Provides installation and registration instructions for Symantec Threat Isolation software and components. It includes a description of the various Symantec Threat Isolation deployment topologies.
- Chapter [4 "Configuring Security Policy Settings"](#) – Describes the building blocks of the Symantec Threat Isolation system and how the organization's administration configures Symantec Threat Isolation system policy settings and rules to support the protection scenarios.
- Chapter [5 "High Availability and Load Balancing"](#) – Describes how Symantec Threat Isolation ensures High Availability (HA) and Load Balancing (LB) across multiple levels of components.
- Chapter [6 "Reports"](#) – Describes activity logging, analytics, and report generation available to the Management user.
- Chapter [7 "Monitoring"](#) – Describes event logs for system events, metric thresholds for tracking logged events, and monitor groups for selecting metric thresholds and Threat Isolation Gateways, setting up email alerts, and defining external servers to which event logs can be forwarded.
- Chapter [8 "User Experience"](#) – Describes differences between the standard interaction of the browser and the alternative interaction that the end user experiences when using Symantec Threat Isolation.
- Chapter [9 "Troubleshooting"](#) – Describes common issues that might be experienced when using Symantec Threat Isolation, related error messages and their meaning, and tools to help troubleshooting the issues.



This document is intended for system administrators who are responsible for installing, integrating, configuring, and maintaining the Symantec Threat Isolation system for use on-premises at customers' sites.

1.4 References

For background information (for example, the Symantec Threat Isolation Platform data sheet and additional product information), refer to:

<https://www.symantec.com/products/web-isolation>

1.5 Terminology

The following terms are used throughout this document.

Table 1 Terminology

Term	Definition
AD	Active Directory (Microsoft)
AD FS	Active Directory Federation Services (Microsoft)
API	Application Program Interface
AWS	Amazon Web Services
C&C	Command and Control
CEF	Common Event Format
CLI	Command Line Interface
CPL	Content Policy Language
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DB	Database
DMZ	Demilitarized Zone
DNS	Domain Name Server
DOM	Document Object Model
DRM	Dynamic Rendering Mode
FQDN	Fully Qualified Domain Name
GIN	Global Intelligence Network
GPO	Group Policy Object (associated with Active Directory)
GRM	Grid Rendering Mode



Term	Definition
HDPI	High Dots Per Inch
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
HTTP/S	HTTP Secure
IDP/IdP	Identity Provider
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MS	Microsoft
NAT	Network Address Translation
NGFW	Next-Generation Firewall
NPLP	Network Protection Licensing Portal
OCSP	Online Certificate Status Protocol
OS	Operating System
PAC	Proxy Auto-Configuration (file)
PDF	Portable Document Format
PDP	Policy Distribution Point
REST	REpresentational State Transfer
SIEM	Security Information and Event Management
SQL	Structured Query Language
SSL	Secure Socket Layer
SAML	Security Assertion Markup Language
Gateway	Threat Isolation Gateway
STIP	Symantec Threat Isolation Platform
SWG	Secure Web Gateway
TBD	To Be Defined
TIE	Threat Isolation Engine
URL	Uniform Resource Locator
VRM	Vector Rendering Mode
XSS	Cross-Site Scripting



2 Symantec Threat Isolation Solution Overview

2.1 Goals and Scenarios

The Symantec Threat Isolation solution has two primary goals and scenarios:

- Protecting an organization's end users and devices from threats, such as malware, that are present while surfing the Internet
- Protecting an organization's web applications from attack by malicious actors, or from abuse by malicious or compromised end users

Protecting the organization's end users from malware

The Symantec Threat Isolation solution protects end users and the organization's enterprise network from attacks, by:

- Isolating websites, emails, and documents so that no malicious content can ever reach the endpoint
- Preventing malware, phishing, and fraud
- Protecting against drive-by infection, malvertising, and ransomware
- Blocking malware Command & Control (C&C), and exfiltration communication

This is achieved by converting the original content into a harmless visual feed through an action called isolation, while retaining the full user experience of full access to websites. This allows organizations to offer a more permissive security policy, since they no longer need to recognize whether or not a website is risky, and thus increases productivity and decreases operational costs.

Protecting the organization's applications

The Symantec Threat Isolation Platform protects web applications by eliminating direct access to the underlying application logic. The Symantec Threat Isolation application does this by:

- Preventing access from bots, as well as brute force and automated attacks
- Eliminating application-level attacks such as Cross-Site Scripting (XSS) and SQL injection
- Blocking client-side script manipulation or HTML manipulation attacks
- Preventing man-in-the-browser and other session hijacking or automated transaction malware compromising legitimate users
- Denying direct access to back-end APIs
- Protecting from infrastructure, server, and operating system vulnerabilities



This is done by presenting the application to the user as a visual feed rather than providing the direct web content of HTML, CSS, Flash, and so on. Direct interaction through HTTP/HTTPS with the site is impossible, meaning that all automated attacks will fail.

2.2 Returned HTML Content

When the end user browses to a website, the matched rule determines which of the following actions will be performed:

- Isolate or Block

In this case, Symantec Threat Isolation returns the Symantec Threat Isolation block page: index.html. The Symantec Threat Isolation block page does not display the original website content, but contains Symantec Threat Isolation client-side logic for initiating WebSocket, sending user gestures, and getting isolated data in return.

Note

The Symantec Threat Isolation block page must not be confused with the application-level block page explained in section [4.4.6 "Creating Custom Pages"](#). The block page described in that section displays HTML content the end user sees when browsing to a website that is blocked in accordance with your company policy (for example, a sports website).

- Pass or Inspect

In this case, Symantec Threat Isolation returns the original HTML content of the website.

2.3 High-level Data Architecture

Symantec Threat Isolation is a clientless solution that enables the organization's end users to safely browse the Internet on any device using any supported browser (for more information about then supported browsers, see section [3.3.1 "Management Browser"](#)). Its zero footprint ensures no need for software installation at the client.

The figure [Symantec Threat Isolation High-Level Data Architecture](#) illustrates the high-level flow of data through the Symantec Threat Isolation Platform.

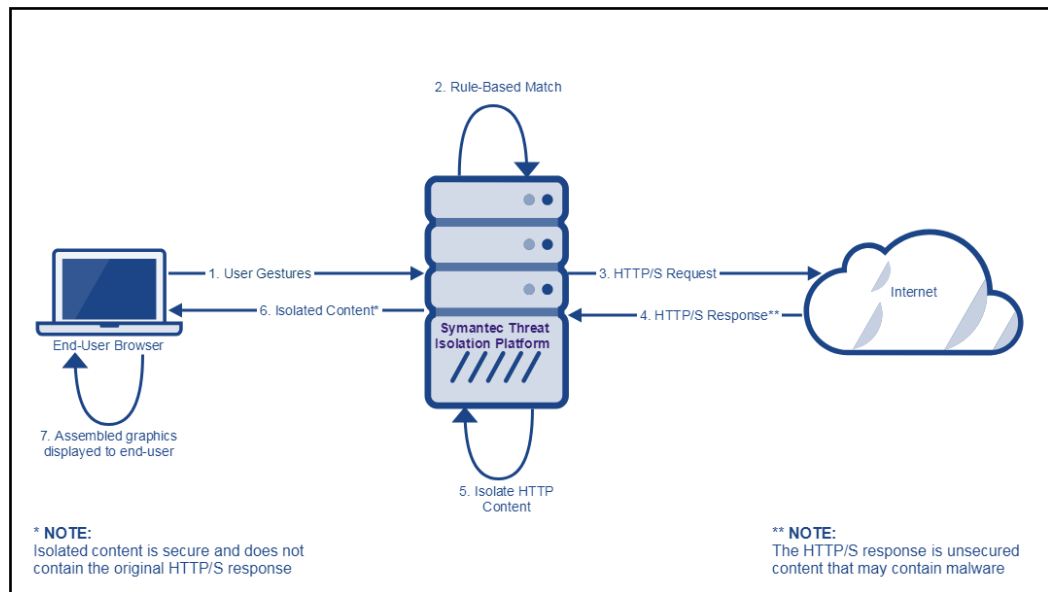


Figure 1 Symantec Threat Isolation High-Level Data Architecture

Data Flow

The following steps describe the flow of data through the Symantec Threat Isolation Platform:

1. Each end-user gesture (that is, mouse clicks, key presses, and changes made to the address bar) are captured in the endpoint browser. This output is captured and transmitted to the Symantec Threat Isolation Platform by WebSocket commands to ensure that only legitimate transactions, initiated by real end users, are performed.
2. The Symantec Threat Isolation Platform translates the end-user gestures and runs the rule-based policy on them.
3. After the rule-base decisions have been determined, when necessary, the Symantec Threat Isolation Platform generates the HTTP/S requests and transmits them to the website.
4. The Symantec Threat Isolation Platform receives the HTTP/S responses. For each element in the webpage, the Symantec Threat Isolation Platform performs a rule-based check against the organization's security policy to determine whether or not to allow the element's isolation and transmission to the end user.
5. If allowed, the Symantec Threat Isolation Platform isolates each element as a separate visual element.
6. The Symantec Threat Isolation Platform transmits the visual elements to the endpoint browser using a proprietary Symantec Threat Isolation protocol.



7. The endpoint browser assembles all the visual elements in their correct locations in the webpage canvas, and displays the isolated webpage to the end user. The Symantec Threat Isolation Platform also returns updated information for subsequent end-user requests or whenever webpage data changes.

2.4 Platform Components

Depending on your deployment topology, you will install most or all of the Symantec Threat Isolation Platform components described in the tables below.

Note

When this guide refers to the Symantec Threat Isolation Gateway ("Gateway"), it refers to a physical gateway that runs both Threat Isolation Engine (TIE) and Threat Isolation Proxy components.

Physical Components:

Component	Functions
Symantec Threat Isolation Management	<ul style="list-style-type: none">■ Defines, manages, and distributes the central security policy to the Threat Isolation Engines (TIEs)■ Required component in all deployment topologies
Threat Isolation Gateway	<ul style="list-style-type: none">■ Terminates the security policy■ Required component in all deployment topologies

Logical Components:

Component	Functions	Resides on
Report Server	<ul style="list-style-type: none">■ Resides on the Symantec Threat Isolation Management machine■ Stores and indexes log data and produces reports	Management
Threat Isolation Engine (TIE)	<ul style="list-style-type: none">■ Isolates incoming HTTP/S requests and responses from the Internet, and passes isolated content to the endpoint browser as a visual stream■ Runs rule base on HTTP/S requests■ Required component in all deployment topologies	One or more Gateways
Threat Isolation Proxy	<ul style="list-style-type: none">■ Authenticates end users, and runs rule base on HTTP/S requests■ Handles HTTP/S requests that do not require isolation and transfers responses to the endpoint■ Not relevant to the Web Application Isolation mode (see section 2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode")	One or more Gateways



Component	Functions	Resides on
Policy Distribution Point (PDP)	<ul style="list-style-type: none">■ Logical component residing on one or more Gateways■ Relays control messages between the Gateways■ The Management server, Threat Isolation Proxy and TIE Gateways must all have access to the PDP. Once these Gateways are interconnected through the PDP, the following takes place above this network:<ul style="list-style-type: none">◆ Management distributes the policy to all Gateways through the PDP◆ The Gateways synchronize live authorization information through the PDP, allowing the TIEs to determine group claims (relevant to both Active Directory and SAML authentication)■ By default, the PDP resides on the first TIE that you register. IMPORTANT: If the PDP is enabled on a Threat Isolation Proxy Gateway, the TIE Gateways will have to access the Threat Isolation Proxy. To avoid this, for security best practice it is recommended to enable the PDP on a TIE Gateway.■ Required component in all deployment topologies	<ul style="list-style-type: none">■ In on-premises deployments, the PDP typically resides on the TIE Gateway (in the DMZ)■ In cloud deployments, the PDP resides on the Management component

2.5 Protection Scenarios

2.5.1 Overview

The Symantec Threat Isolation solution provides two main protection scenarios:

- [Protecting an Organization's Endpoints from Attack](#) – This protection scenario protects an organization's end users and devices from threats, such as malware^[1], that are present while surfing the Internet. In this scenario, Symantec Threat Isolation isolates all HTTP/S traffic to and from the Internet and converts the original content into harmless visual elements. For more information, see section [2.5.2 "Protecting an Organization's Endpoints from Attack"](#).

[1] For more information, see the Wikipedia description of malware at: <https://en.wikipedia.org/wiki/Malware>.



- [Protecting an Organization's Web Applications from Attack](#) – This protection scenario protects an organization's web applications from attacks and from abuse by malicious or compromised end users. In this scenario, Symantec Threat Isolation eliminates direct access to the underlying application logic. For more information, see section [2.5.3 "Protecting an Organization's Web Applications from Attack"](#).

2.5.2 Protecting an Organization's Endpoints from Attack

Symantec Threat Isolation protects your organization's endpoints from malware, that is, malicious software designed to damage endpoint computers.

The system offers complete protection to end users with regard to the following:

- Webpages - Symantec Threat Isolation protects against drive-by malware attacks that occur when end users browse webpages. The system provides an out-of-the-box policy that enforces isolation of all HTTP/S traffic to and from the Internet. It renders isolated webpages as visual elements or streams in the endpoint browser, thus preventing malware from ever reaching the client side. Since the Threat Isolation Engine (TIE) handles all communication with web servers, the endpoint browser is completely protected.
- Downloaded files - Symantec Threat Isolation scans files that are downloaded from webpages as defined in the security policy's Download Profile. The downloaded files are inspected for malware and manipulated or sanitized before being transferred to the end user. Only clean, isolated files are transferred to the end user.



Organizations today might use sophisticated content scanning techniques, such as sandboxing, which are performed in parallel with the download. When such techniques are used, the administrator is notified of malware only after the malware has already passed through. This is because these methods take time to run and often require access to the complete file. By the time content scanning is completed, the connection to the end user will have timed out.

In contrast, Symantec Threat Isolation fully downloads the file to the Threat Isolation Gateway and performs the necessary security measures before starting the connection to the end user, thus eliminating any time limitation. This allows Symantec Threat Isolation to integrate with sophisticated techniques (including the use of network sandboxes[1], file sanitization[2], or prompting the user for a password for an encrypted zip-file) that cannot be integrated in real-time in other solutions.

- Links in email - Symantec Threat Isolation isolates links contained in email by rewriting them so that the end user is redirected to an Isolation Portal. In this mode, the isolated link consists of the name of the Threat Isolation Gateway and a parameter holding the original URL.
- Applications - Symantec Threat Isolation offers the granularity to protect end users when non-browser applications are used. Such applications are native applications that use the HTTP protocol even though they are not browsers; for example, Microsoft Office and Slack. Out of the box, Symantec Threat Isolation enforces a Pass rule for a predefined list of applications. It also provides a closure Pass rule for all other applications, in order to avoid connectivity issues in your organization. It is good practice to manually change the closure Pass rule to Block and then add the applications that your end users use and that are permitted by your organizational policy to the Pass rule, so that only those applications will pass, while all others are blocked.
- Bots are broken. When an application is isolated, a bot script cannot receive the original response from the server and therefore cannot communicate with it.

[1] A sandbox is an isolated computing environment in which a program or file can be executed without affecting the application in which it runs. (See <http://searchsecurity.techtarget.com/definition/sandbox>.)

[2] [File] sanitization is the process of ensuring that only the intended information can be accessed from a document. [This process] includes removing document metadata (e.g., changes, history, or other text or code inserted as part of the metadata) that could pose a ... security risk. (See <http://whatis.techtarget.com/definition/document-sanitization>.)



2.5.3 Protecting an Organization's Web Applications from Attack

In addition to protecting your organization's endpoints, Symantec Threat Isolation protects your organization's website, web applications in the Cloud, and any internal applications that might contain sensitive information; these can be vulnerable to malicious end users or users compromised with malware that allow a third-party attacker access to sensitive information.

- Symantec Threat Isolation isolates web applications from end users. The system transforms content into visual elements, so that users can no longer interact directly with the website back end (by submitting HTTP posts or using APIs) or view the site's source code, logic, or origin from which third-party content comes. Only user gestures through WebSocket commands are transmitted from the client side to the Threat Isolation Engine (TIE). The website's client-side logic runs on the Symantec Threat Isolation Platform and cannot be bypassed by attackers.
- All of your organization's web applications are isolated and presented as visual elements. The end user cannot view the original application code.
- Security administrators control what information leaves the application. Operations such as copy/paste, saving files or images, and printing can be controlled and logged. Downloading application files by end users can be blocked. The TIE tracks all user gestures and eliminates any data leakage resulting from mouse and keyboard actions.

2.6 Deployment Topologies

2.6.1 Overview

Symantec Threat Isolation can be deployed in any of the following topological models. Each topology is described in detail in the following sections. Note that all of these topologies support dynamic load balancing.

The following topologies protect your organization's endpoints from attack:

- Symantec Threat Isolation Explicit Proxy – See section [2.6.2 "Symantec Threat Isolation Explicit Proxy"](#)
- Symantec Threat Isolation with Downstream Proxy Forwarding – See section [2.6.3 "Symantec Threat Isolation with Downstream Proxy Forwarding"](#)
- Symantec Threat Isolation with Block Page Integration – See section [2.6.4 "Symantec Threat Isolation with Block Page Integration"](#)
- Symantec Email Threat Isolation – See section [2.6.5 "Symantec Email Threat Isolation"](#)



The following topology protects your organization's web applications from attack:

- Symantec Threat Isolation as Web Application Isolation Gateway Mode – See section [2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode"](#)

2.6.2 Symantec Threat Isolation Explicit Proxy

In this topology, all components belong to the Symantec Threat Isolation Platform, and Symantec Threat Isolation functions as a proxy.

In this topology, the organization's endpoints communicate directly with the Threat Isolation Proxy. Isolation and inspection of SSL traffic on the organization's network is provided by deployment of CA certificates that are held by the Proxy. The web server's original responses to HTTP/S requests never reach the client; all HTTP/S responses are provided to the endpoint as isolated content. The Proxy handles content blocking (for an explanation of the Symantec Threat Isolation block page, see section [8.6 "Block Page"](#)), as well as standard communication with web servers for Pass webpages.

This topology requires minimal configuration on the endpoint browser, which is easily deployed through GPO.

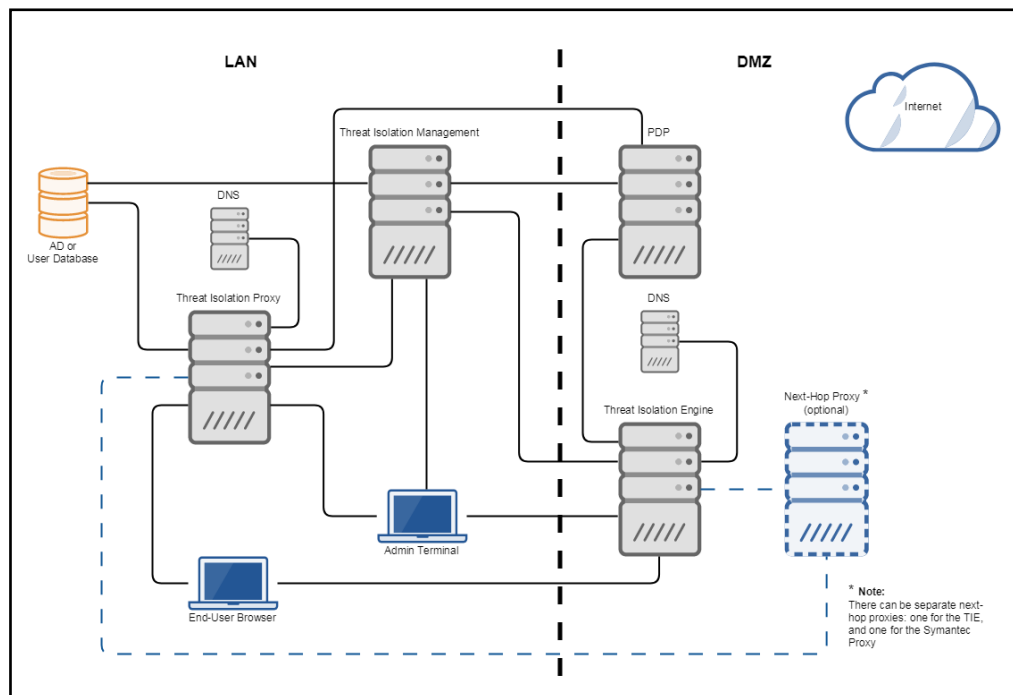


Figure 2 Symantec Threat Isolation Explicit Proxy



2.6.3 Symantec Threat Isolation with Downstream Proxy Forwarding

In this topology, the organization's endpoints communicate indirectly with the Threat Isolation Proxy through a downstream proxy.

Isolation and inspection of SSL traffic on the organization's network is provided by deployment of CA certificates that are held by the downstream proxy. If the downstream proxy supports policy-based forwarding, it is responsible for endpoint communication with the Threat Isolation Proxy and the Threat Isolation Engine (TIE); the downstream proxy decides whether or not to forward.

It is recommended to use the Symantec Secure Web Gateway (ProxySG) as your downstream proxy. As products from the same vendor, Symantec Threat Isolation and Symantec ProxySG can be integrated smoothly. This convenience is not available when using any other product.

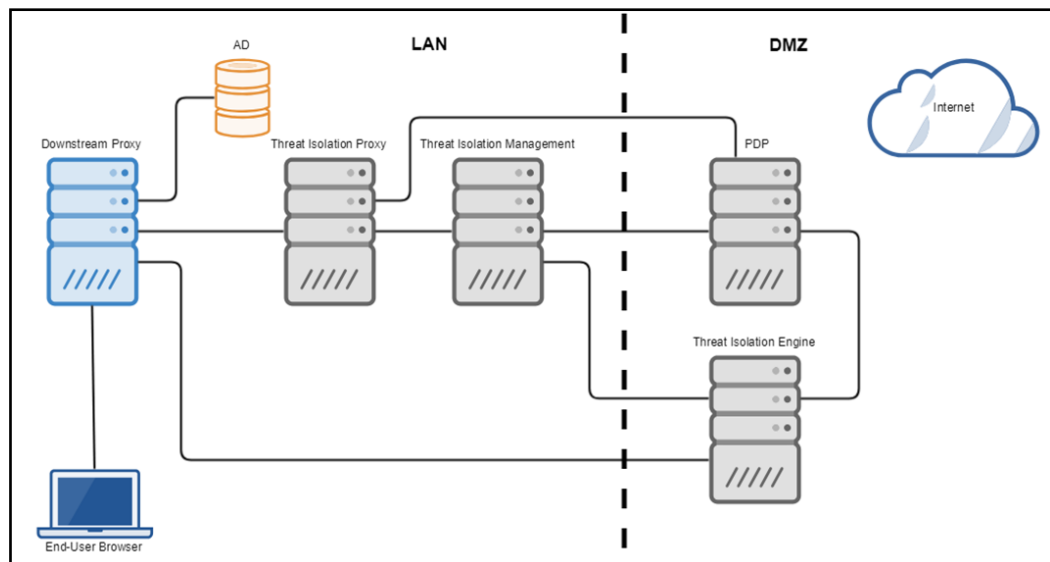


Figure 3 Symantec Threat Isolation Integrated with a Downstream Proxy

If your organization's downstream proxy cannot forward traffic, it is recommended to implement the Block Page Integration topology. For more information, see section [2.6.4 "Symantec Threat Isolation with Block Page Integration"](#).

2.6.4 Symantec Threat Isolation with Block Page Integration

When a next-generation firewall (NGFW) or a Secure Web Gateway (SWG) that cannot selectively forward traffic to the Isolation Platform resides between the organization's endpoints and the Isolation Platform, the downstream proxy topology is not applicable. In this case, there are several possible solutions:



- The NGFW forwards all traffic to the Symantec Threat Isolation Platform.
- The NGFW/SWG redirects traffic to the Isolation Portal. This solution has the following limitations: The Content Security Policy[1] might not allow resources to be redirected, and subresources of (non-isolated) bypassed webpages might be incorrectly redirected to the Isolation Portal. If your organization's NGFW/SWG has redirected traffic to a block page before, you can decide which of the blocked websites should now be isolated instead of blocked, and change their redirect URL from that of the block page to that of the Isolation Portal. This topology is recommended for use with specific URLs and uncategorized websites.

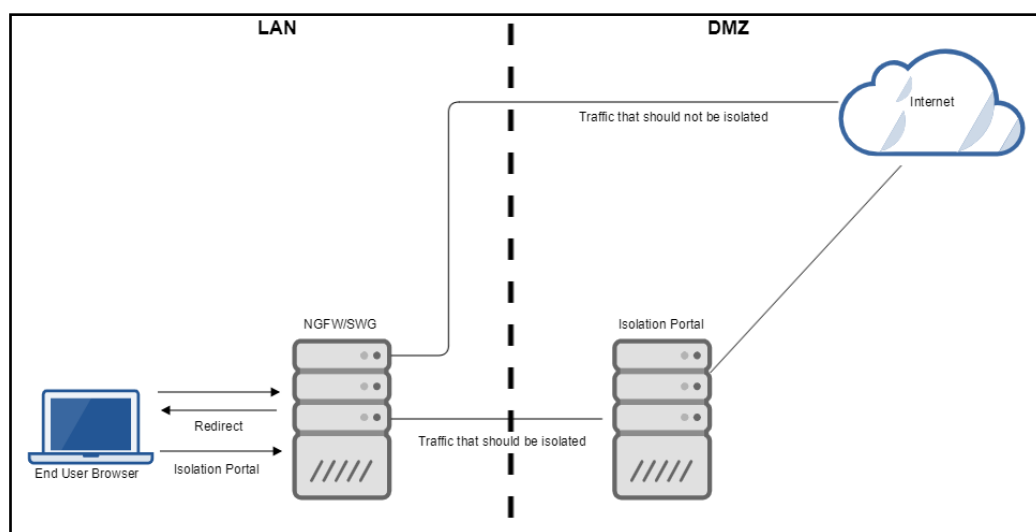


Figure 4 Symantec Threat Isolation with Block Page Integration

- A transparent SWG (such as Symantec ProxySG) with selective forwarding capability is placed between the NGFW/SWG and the Symantec Threat Isolation Platform. The transparent proxy selectively forwards specific categories to the Isolation Platform. This topology is also recommended for use with categorized websites, such as social networks, which typically use Content-Security-Policy[2].

[1] For more information, see <https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP>.

[2] For more information, see the Wikipedia description of Content-Security-Policy at: https://en.wikipedia.org/wiki/Content_Security_Policy.

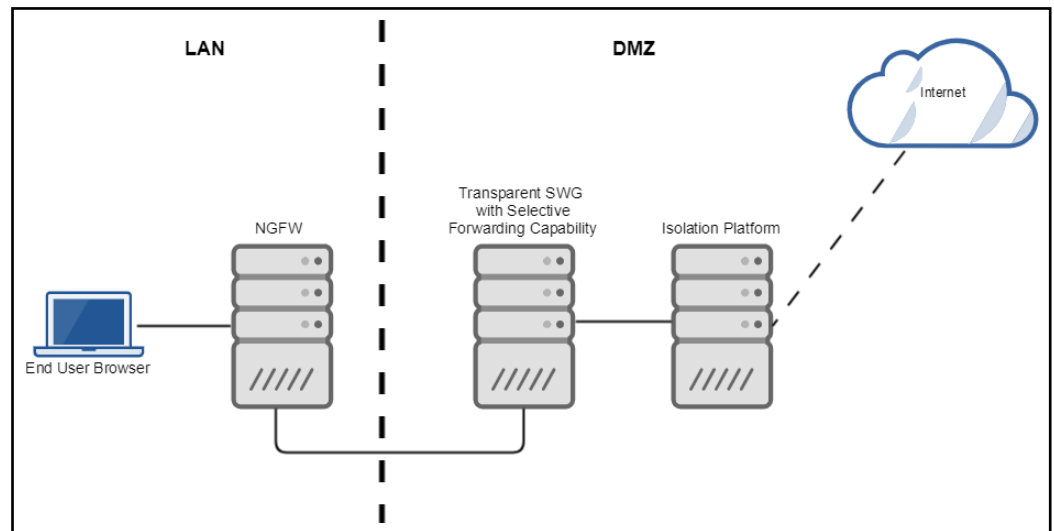


Figure 5 Symantec Threat Isolation with Transparent SWG

2.6.5 Symantec Email Threat Isolation

This topology protects email recipients from emails containing links to high-risk and phishing websites. There are two deployment options:

- **ESS Integration** - Symantec Threat Isolation can be integrated with Symantec's Email Security Services (ESS) solution. In this topology, organizations that use ESS select "Isolation" in the ESS console, which causes inbound emails to be scanned and all links to be rewritten. When the email recipient clicks the link, Email Threat Isolation returns an address based on the risk level of the website to which the link points (either the default risk level, or the custom risk level the organization wants to isolate). If the website must be isolated, the returned URL will be that of the Isolation Portal, so that the requested website is isolated. Typically, the hostname is email-isolation.prod.fire.glass. Note that Email Threat Isolation serves only links that were rewritten and signed by ESS. Otherwise, the URL is not considered valid.
- **SMG Integration** - Symantec Threat Isolation can be integrated with the Symantec Messaging Gateway (SMG). In this topology, when an email message contains a malicious link according to the SMG's policy criteria, SMG will rewrite the link. The rewritten link consists of the hostname of the Isolation Portal and a parameter containing the original URL. Therefore, when the email recipient clicks the link, the requested website is isolated. The Isolation Portal can reside on an on-premises server, or on a server in the cloud so that it is accessible to roaming users from anywhere in the world.



Note that in the Symantec Email Threat Isolation topology, the Isolation Portal does not use authentication. Instead, the Email Threat Isolation API signs the URL with a token string appended to the URL. Once the isolation instance has verified the token, it gives the client a session cookie used for authorization. When Symantec Threat Isolation is integrated with ESS, the Threat Isolation Gateway comes configured to use token authorization. However, if the system is integrated with SMG, you must configure the Gateway to use it.

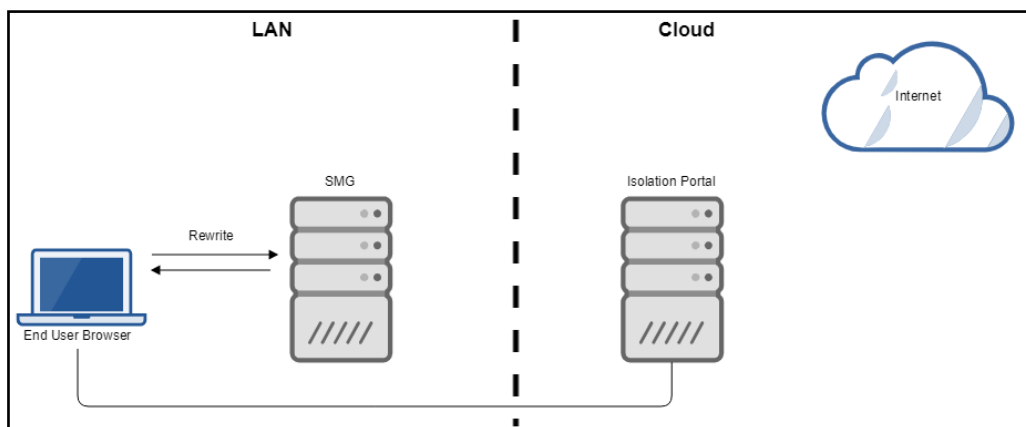


Figure 6 Symantec Threat Isolation with SMG

For information about configuring the Symantec Email Threat Isolation topology, see section [3.6.4 "Configuring Symantec Email Threat Isolation"](#).

When the SMG rewrites a link's URL, the rewritten URL uses this format:

```
https://<isolation-portal-host>/smg/<version>?url=<target_url>&metadata=<metadata>&sig=<sig>
```

where:

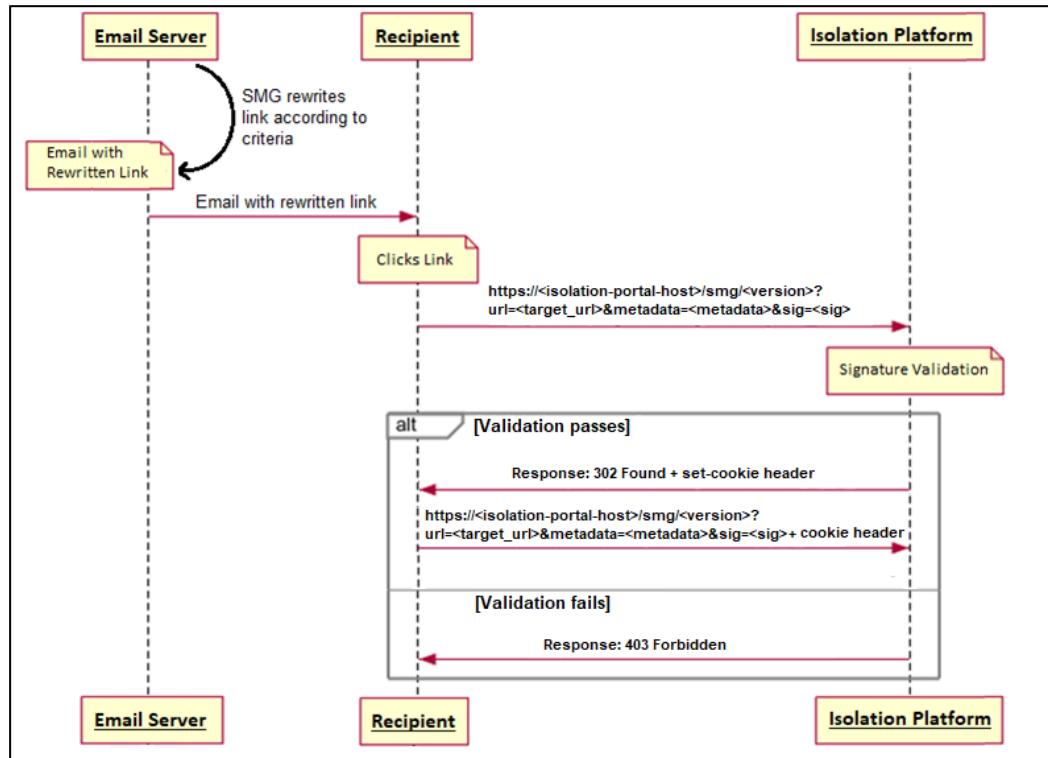
- <isolation-portal-host> is the name of the Isolation Portal
- <version> is the version number of the SMG library (the current version is 1)
- <target_url> is the original URL
- <metadata> is the metadata that SMG sends to the Isolation Portal
- <sig> is a signature that proves to the Threat Isolation Engine (TIE) that the URL was signed by an SMG instance

When the Isolation Platform receives the request, it validates the signature, sets a session cookie in the response to the client, and redirects it to the following URL:

```
https://<isolation-portal-host>?url=<target_url>
```



The isolated link consists of the Isolation Portal hostname and a parameter holding the original URL. The following diagram illustrates the flow in Symantec Email Threat Isolation mode.



1. An email with a link is sent to a recipient.
2. SMG rewrites the link according to the policy.
3. The recipient receives the email and clicks the rewritten link.
4. The new URL points to the Isolation Platform.
5. The Isolation Platform validates the signature and sets a signed cookie in the response 302 Found to the email recipient.
6. The Isolation Platform redirects to a simpler URL, without the signature but with the cookie.
7. The Isolation Platform makes sure the received cookie is valid and was set by itself (in step 5).
8. One of the following happens, depending on the outcome of the validation:
 - ◆ If the validation passes, the email recipient will browse the requested website in the Isolation Platform.



- ◆ If the validation fails (that is, the signature data that SMG signed is not valid), the Isolation Platform will send a response 403 Forbidden.

2.6.6 Symantec Threat Isolation as Web Application Isolation Gateway Mode

In this topology, only the Threat Isolation Engine component is active in the Symantec Threat Isolation Platform. This topology protects the organization's web applications, rather than its endpoints, from attack by eliminating direct access to the underlying application logic:

- Grid rendering mode (GRM) hides DOM elements, CSS, internal logic and API calls from the client. It displays the browser content as images to the client. This mode utilizes high bandwidth.
- Vector rendering mode (VRM) hides internal logic and API calls from the client (no JavaScript runs on the endpoint browser). It displays only HTML visual elements (DOM elements and CSS).

The Symantec Threat Isolation Platform can also block the downloading of the organization's application files by end users.

2.6.6.1 Using a Load Balancer

The Symantec Threat Isolation as Web Application Isolation Gateway Mode topology can be deployed with a third-party load balancer that distributes traffic among multiple Threat Isolation Gateways sharing the same DNS name. The load balancer should ensure that stickiness is maintained when all Threat Isolation Engines (TIEs) have the same Public DNS name.

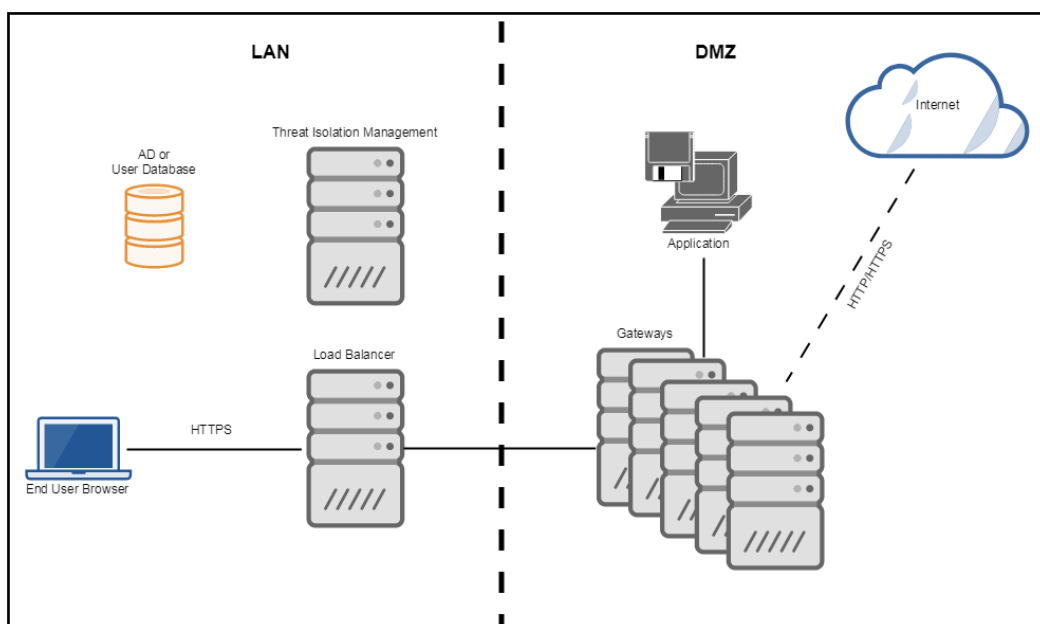


Figure 7 Symantec Threat Isolation as Web Application Isolation Gateway Mode with a Load Balancer

When an end user browses to the application and then opens another connection, the load balancer should ensure that an isolation channel opened from the same endpoint browser stays with the same TIE. This precludes having to open a new session. The load balancer must support WebSocket. For more information, see section [4.7.7.2 "Enabling Web Application Isolation Gateway Mode with a Load Balancer"](#).

2.6.6.2 Not Using a Load Balancer

When your organization does not use a load balancer to ensure that stickiness is maintained when all Threat Isolation Gateways share the same Public DNS name, stickiness must be achieved in another way. In this scenario, Symantec Threat Isolation enables you to configure the Threat Isolation Engines (TIEs) to listen to WebSocket requests by their unique hostname rather than by a single shared Public DNS name. In this case, WebSocket will always be opened to the same TIE on the same Gateway, thus achieving stickiness. The TIE will still listen to the Public DNS name for returning the index.html block page. For more information, see section [4.7.8.1 "Enabling Web Application Isolation Gateway Mode - No Load Balancer"](#).

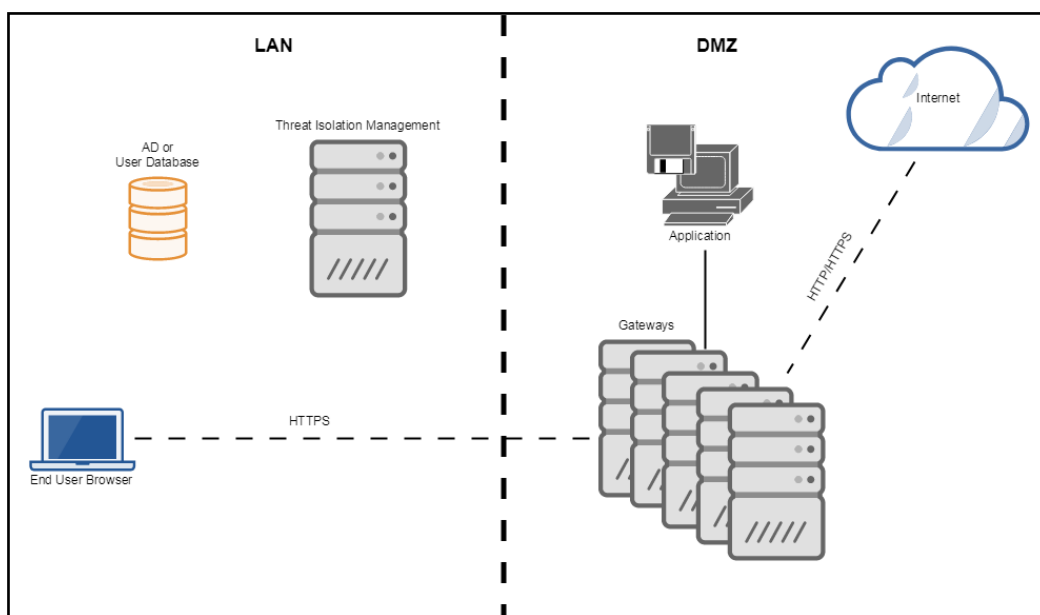


Figure 8 Symantec Threat Isolation as Web Application Isolation Gateway Mode without a Load Balancer

2.7 Cloud Services

Some Threat Isolation Gateway logic depends on access to the Internet for regular updates, for example with regard to URL categorization, updating the web browser on the server side, enabling feedback, and more. For this purpose, the Gateway consumes cloud services. This is done securely over SSL.

For all relevant information about cloud services consumed by the Gateways, contact Symantec Threat Isolation technical support.

2.8 How Symantec Threat Isolation Processes Private Data

To achieve complete isolation, full protection of the endpoint, and an optimal user experience, Symantec Threat Isolation processes content on the Threat Isolation Gateway.

Private data that is sent from the endpoint machine to the Gateway is secured. However, some private data such as cookies and downloaded files must reside on the Gateway (which can be an on-premises server or a cloud server, depending on your topology). Cookies never leave the Gateway machine and never reach the client. Downloaded files briefly reside on the Gateway for scanning purposes, before reaching the client. Uploaded files are sent from the client to the Gateway, where they reside briefly for upload profile policy purposes.



The following sections detail how Symantec Threat Isolation processes the end user's private data.

2.8.1 Cookies and Session Data

When an end user browses to an isolated website for the first time, the Threat Isolation Engine (TIE) creates an instance of the browser on the TIE that contains no cookies or persistent data. Symantec Threat Isolation saves such data, and any cookies that were created as a result of the isolated browsing session, locally on the TIE. The cookies are encrypted and stored separately per random identifier that is unique per user and browser, so that no data can leak between users or between different browsers with the same user.

Symantec Threat Isolation does not save the unique random identifier used for storing the cookies on the TIE; it is saved only on the endpoint browser, and only the user can access these cookies.

2.8.2 Browsing Logging Data

Symantec Threat Isolation collects and stores browsing data only for the following purposes:

- Error reporting (see section [3.5.7 "Defining the Management Gateway"](#)). Error logs are reported to Symantec Threat Isolation technical support.
- Creating activity logs (see section [4.3.6 "Defining Activity Log Profiles"](#)). Activity logs are *not* reported to Symantec Threat Isolation technical support.

You can enable, disable and configure this functionality from the Management UI.

Browsing logging data can include the following:

- For error reporting:
 - ◆ URLs for websites and resources the user has browsed
 - ◆ The user's IP address
 - ◆ The user's username
- For Activity Logs:
 - ◆ URLs for websites and resources the user has browsed
 - ◆ User activity, including keyboard and clipboard data, mouse gestures and metadata of network requests
 - ◆ Authentication metadata
 - ◆ The user's IP address



- ◆ The user's username

Note

By default, HTTP query parameters are removed from the URLs for privacy.

2.8.3 Cloud Telemetry Data

Symantec Threat Isolation collects anonymous telemetry data from its servers. This information is uploaded to the third-party cloud platforms <https://www.datadoghq.com/> and <https://www.splunk.com/> for error reporting, monitoring and troubleshooting purposes. You can disable this functionality in the First Time Wizard (see section [3.5.7 "Defining the Management Gateway"](#)).

Cloud telemetry data can include:

- Threat Isolation Gateway hostname and IP address
- Threat Isolation Gateway performance counters, including network, disk, memory and CPU
- Custom Threat Isolation metrics, including number of open tabs, URLs the user has browsed, and user experience, responsiveness and load-time metrics
- Threat Isolation Engine (TIE) errors, which might include data such as the user's IP address, URLs the user has browsed and username

All private data obtained from the TIE gateways is anonymized.

Note

By default, HTTP query parameters are removed from the URLs for privacy.

2.8.4 Third-Party File Sanitizer Data

Symantec Threat Isolation might send files that the user downloaded during an isolated session to a configured file sanitizer (on-premises or Cloud) for scanning and sanitizing purposes.

File sanitizers can include:

- OPSWAT Metadefender Cloud
- VirusTotal
- Votiro SDS API 3.0
- Google Safe Browsing

To enable, disable and configure this functionality, go to:

Profiles → Download Profiles → Advanced Settings



For more information, see section [4.3.4 "Defining Download Profiles"](#).

2.8.5 Document Viewer Data

Symantec Threat Isolation might send files that the user downloaded during an isolated session to a Symantec cloud server on the Amazon Web Services (AWS) platform for remote document-viewing purposes. You can enable, disable and configure this functionality from the Management UI (see section [4.3.4.2 "Document Isolation Viewer"](#)).

After a file is uploaded to the Symantec cloud server, the isolation platform creates a unique token for that file. The Threat Isolation Engine (TIE) can only access this token for this specific user's session. Files reside encrypted in the cloud storage and are deleted from it automatically every day.

2.8.6 Flash Activation Request Data

Symantec Threat Isolation sends Flash Activation requests issued from an end user browsing isolated websites to a Symantec AWS cloud server. Every request collects the URL and IP address of the Threat Isolation Engine (TIE) that issued the request. No data associating the end user to the request is collected. Symantec Threat Isolation sends all such data using an encrypted connection and secured credentials.

2.9 Reducing Bandwidth Usage

Symantec Threat Isolation significantly reduces the amount of bandwidth used on the client side.

When an endpoint user browses directly to a website to retrieve content, the browser consumes a certain amount of bandwidth. When a web page is isolated using Symantec Threat Isolation, web traffic to this webpage is handled by the Threat Isolation server.

The Threat Isolation platform uses bandwidth reduction heuristics to streamline the content being transferred to the endpoint, thus decreasing bandwidth usage. In Cloud deployments, where the Isolation gateway is further away from the endpoint, this is particularly significant.

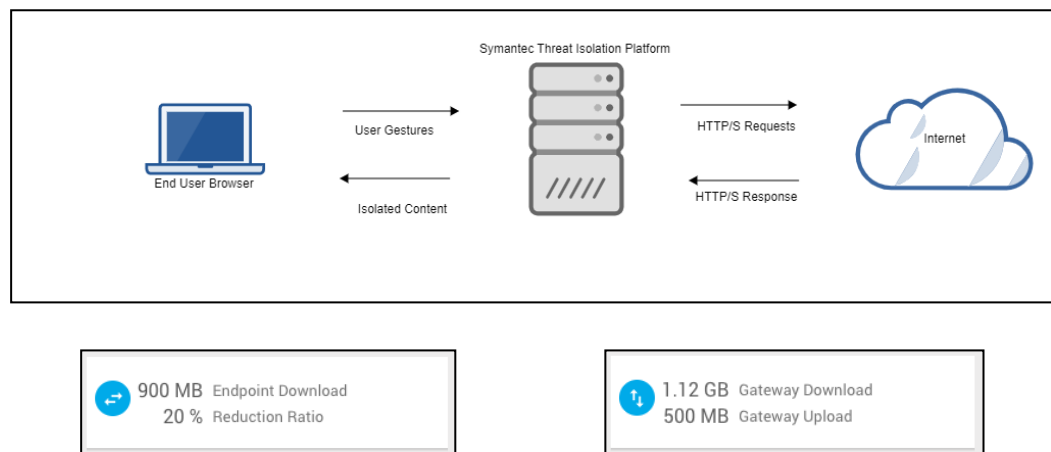
The platform also uses a granular policy to decrease bandwidth consumption by configuring the media quality settings for the endpoint. You can change the settings for images, video files and audio files to save considerable bandwidth. For changing Media Quality settings to reduce bandwidth usage, see section [4.3.3.2 "Adding an Isolation Profile"](#).



As a result of these capabilities, the endpoint will consume less bandwidth when using the isolation platform than a browser in a non-isolated set-up downloading content directly from the website.

The exact bandwidth used by the endpoint browser and the isolation gateway browser are logged in the Activity Logs.

Analytics uses widgets to summarize and visualize the information displayed in the Activity Logs.



Reduction ratio represents the percentage of download bandwidth saved.

For isolated sessions, the default endpoint bandwidth usage logging interval is 3600 seconds. You can configure the interval using the `bandwidth_usage_collection_interval` setting. The minimum interval is 60 seconds.

The session is also logged when it ends.

3 Installing the Symantec Threat Isolation Platform

3.1 System Requirements

IMPORTANT!

Installing the Symantec Threat Isolation Platform includes installation of the Linux operating system. Therefore, the Symantec Threat Isolation Platform components must be installed on a barebone machine.



The table below lists the minimum system requirements for the Symantec Threat Isolation machines. These requirements can be expanded according to the number of users in your organization. For more information, contact Symantec Threat Isolation technical support.

Symantec Threat Isolation Platform Component	Disk Space (GB)	CPU (Virtual Cores)	Memory (GB RAM)
Management Gateway and Report Server	256	8	16
Threat Isolation Proxy Gateway	256	8	16
Threat Isolation Engine (TIE) Gateway	256	8	16
Singlebox (Management and Reporting, Proxy and TIE)	512	16	32

3.2 Supported Platforms

The Threat Isolation Gateways can run on the following platforms:

Platform	Description
VMWare ESX	VMWare ESX is an enterprise-level product developed by VMware that is used for server virtualization. It runs without requiring an existing operating system on the physical machine. Note that the virtual machine must have a configured network adapter
KVM	Kernel-based Virtual Machine (KVM) is a physical virtualization infrastructure for the Linux kernel
AWS	Amazon Web Services (AWS) is a subsidiary of Amazon.com that provides on-demand cloud-computing platforms on a paid-subscription basis
Microsoft Azure	Microsoft Azure (formerly Windows Azure) is a cloud-computing service created by Microsoft for building, testing, deploying, and managing applications and services through a global network of Microsoft-managed data centers
Rackspace	Rackspace Cloud Servers is a cloud-infrastructure service that enables users to deploy cloud servers. The cloud servers are virtual machines running on Linux-based instances



3.3 Supported Browsers

3.3.1 Management Browser

Symantec Threat Isolation Management is a web application. The Management browser must support all capabilities Management needs in order to work properly. The table below lists the minimum compatible browser versions.

Browser	Minimum Version
Chrome (recommended)	51
Edge	12
Firefox	47
Internet Explorer	11
Safari	10

3.3.2 Endpoint Browser

The endpoint browser must support all required capabilities relating to the isolation flow. The table below lists the minimum compatible browser versions.

Browser	Minimum Version
Chrome	56
Edge	38
Firefox	54
Internet Explorer	11
Safari	11

The following operating systems are supported:

- Windows 7 and up
- Windows Server 2008 and 2016
- macOS 10.12 Sierra and up
- iOS 12 and up
- Android 8 and up



3.4 Preparing for Symantec Threat Isolation Platform Installation

3.4.1 Overview

Perform the tasks described in the following table in preparation for Symantec Threat Isolation Platform installation.

Task	Description	For More Information
Define Symantec Threat Isolation Platform components	For each machine, define the components that will reside on it: <ul style="list-style-type: none">■ Management■ Report Server■ Threat Isolation Engine (TIE)■ Threat Isolation Proxy■ PDP	■ See section 3.4.2 "Defining Components Per Machine"
Define Networking	Networking tasks include the following: <ul style="list-style-type: none">■ Define locations of all machines on LAN, DMZ, and cloud networks■ Define FQDN IDs NOTE: On a TIE machine, make sure the domain of its FQDN is different than the domain of the organization■ Define IP addresses	■ See section 3.4.3 "Defining Networking" ■ See section 3.4.3.1 "TIE Public DNS Name Considerations"
Define Firewall Rules	Define your firewall rules to ensure communication with Symantec Threat Isolation components	
Define SSL certificates (Certificate Authority /Server Certificates)	Depending on your topology, define root CA keys or one or more server certificates	■ See section 3.4.3.1 "TIE Public DNS Name Considerations" ■ For root CA, see section 3.4.4 "Signing the CA Certificate"

3.4.2 Defining Components Per Machine

Before installing the Symantec Threat Isolation Platform, perform the following machine-related tasks:



1. In consultation with Symantec Threat Isolation technical support, determine the total number of machines needed in your organization.
2. Decide which physical and logical component(s) will reside on each machine:

Physical Components:

Component	Functions
Symantec Threat Isolation Management	<ul style="list-style-type: none">■ Defines, manages, and distributes the central security policy to the Threat Isolation Engines (TIEs)■ Required component in all deployment topologies
Threat Isolation Gateway	<ul style="list-style-type: none">■ Terminates the security policy■ Required component in all deployment topologies

Logical Components:

Component	Functions	Resides on
Report Server	<ul style="list-style-type: none">■ Resides on the Symantec Threat Isolation Management machine■ Stores and indexes log data and produces reports	Management
Threat Isolation Engine (TIE)	<ul style="list-style-type: none">■ Isolates incoming HTTP/S requests and responses from the Internet, and passes isolated content to the endpoint browser as a visual stream■ Runs rule base on HTTP/S requests■ Required component in all deployment topologies	One or more Gateways
Threat Isolation Proxy	<ul style="list-style-type: none">■ Authenticates end users, and runs rule base on HTTP/S requests■ Handles HTTP/S requests that do not require isolation and transfers responses to the endpoint■ Not relevant to the Web Application Isolation mode (see section 2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode")	One or more Gateways



Component	Functions	Resides on
Policy Distribution Point (PDP)	<ul style="list-style-type: none">■ Logical component residing on one or more Gateways■ Relays control messages between the Gateways■ The Management server, Threat Isolation Proxy and TIE Gateways must all have access to the PDP. Once these Gateways are interconnected through the PDP, the following takes place above this network:<ul style="list-style-type: none">◆ Management distributes the policy to all Gateways through the PDP◆ The Gateways synchronize live authorization information through the PDP, allowing the TIEs to determine group claims (relevant to both Active Directory and SAML authentication)■ By default, the PDP resides on the first TIE that you register. IMPORTANT: If the PDP is enabled on a Threat Isolation Proxy Gateway, the TIE Gateways will have to access the Threat Isolation Proxy. To avoid this, for security best practice it is recommended to enable the PDP on a TIE Gateway.■ Required component in all deployment topologies	<ul style="list-style-type: none">■ In on-premises deployments, the PDP typically resides on the TIE Gateway (in the DMZ)■ In cloud deployments, the PDP resides on the Management component

3. Make sure each machine meets the minimum system requirements for the assigned component(s). For more information, see "System Requirements" in section [3 "Installing the Symantec Threat Isolation Platform"](#).

3.4.3 Defining Networking

IMPORTANT!

- Be sure to use static IP addresses. Do *not* use DHCP.
- The Management machine must have access to email and Syslog servers.

Before installing the Symantec Threat Isolation Platform, perform the following networking-related tasks:

1. Define which machines are located in LAN and DMZ networks.
2. Assign an IP address to each machine.
3. Register the FQDNs of all Symantec Threat Isolation machines with your DNS server.

Note

If this is a Threat Isolation Engine (TIE) machine, make sure the domain of its FQDN is different than the domain of the organization before registering it with the DNS server. For more information, see section [3.4.3.1 "TIE Public DNS Name Considerations"](#).



4. Set up the firewall rule base for your deployment topology.

3.4.3.1 TIE Public DNS Name Considerations

When the end user browses to a website and the matched rule is Isolate or Block, Symantec Threat Isolation will return the Symantec Threat Isolation block page: index.html (see section [2.2 "Returned HTML Content"](#)). This page does not display the original website content, but contains client-side logic for initiating WebSocket directed to the Threat Isolation Engine (TIE).

Internet Explorer has a security feature that automatically assigns all websites to one of several security zones, such as Internet and Local intranet. When IE regards a web resource as residing in the Local intranet, and that web resource is part of a website that resides in the Internet, it will block the connection to the Local intranet resource.

IE regards all isolated websites as residing in the Internet security zone. These websites should connect to TIE Gateways, but when IE regards the TIEs as residing in the Local intranet zone, it blocks the connection and a blank page is displayed.

To avoid this issue, do the following:

- Make sure your TIE Gateways have a Public DNS name that is FQDN. For more information, see section [4.7.7 "Defining a Threat Isolation Gateway"](#).

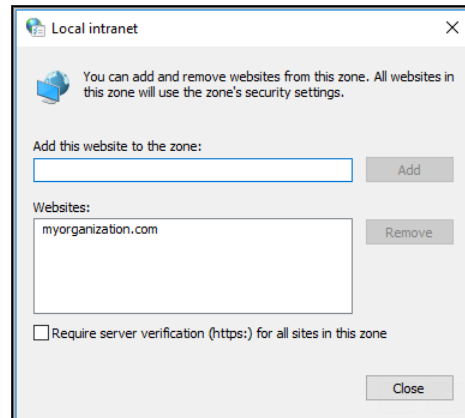
For example, if your organization's domain name is myorganization.com, assign the Public DNS name tie1.myorganization.com to the TIE. IE will now consider the TIE to reside in the Internet zone.

Note that when the TIE's Public DNS Name lacks a domain name, IE will autocomplete the host name with the domain name and consider this host to reside in the Local intranet.

- If the GPO for your organization has defined the FQDN of the TIEs in the Local intranet list explicitly, assign the TIE Gateways to a subdomain.

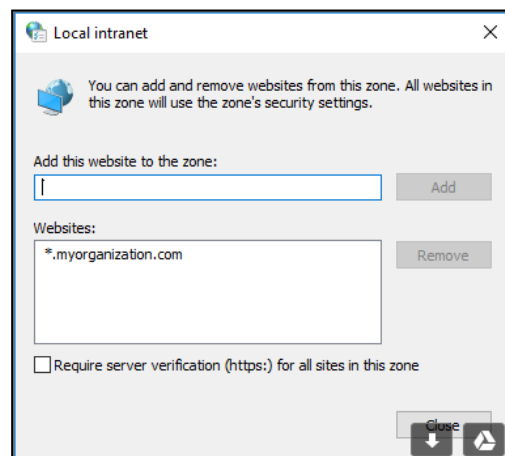


For example, if your organization's domain name is myorganization.com and it is defined in the Local intranet zone, as shown in the figure below, your TIEs will be regarded as residing in the Local intranet.



To avoid this, assign FQDNs to the TIEs as follows:
tie1.isolation.myorganization.com, tie2.isolation.myorganization.com, etc.

If a wildcard domain like *.myorganization.com is defined, IE will regard a TIE with the sub-domain tie1.isolation.myorganization.com as residing in the Local intranet. Create a different domain, such as fictitiousdomain.com, and assign tie1.fictitiousdomain.com, tie2.fictitiousdomain.com and so on to the TIEs. Configure the DNS server to resolve this IP to the TIE's real IP.



For more information, see section [9.3.1.2 "Internet Explorer Does Not Show Isolated Page; Chrome Does"](#).

3.4.4 Signing the CA Certificate

Symantec Threat Isolation uses a CA certificate for the following purposes:



- To sign a server certificate for each website it intercepts: When the Threat Isolation Proxy intercepts SSL traffic, it acts as man-in-the-middle (MITM) and needs a CA to sign server certificates for the websites it intercepts.
- To sign a server certificate for each Threat Isolation Gateway.

Note

It is strongly recommended to sign the CA certificate prior to starting the Symantec Threat Isolation installation process.

In the following topologies, all endpoint browsers in your organization must trust the CA certificate of the Threat Isolation Proxy:

- When there is no proxy between the Threat Isolation Proxy and your organization's endpoint browsers.
- When there is a downstream proxy between the Threat Isolation Proxy and your organization's endpoint browsers, but that downstream proxy does not intercept SSL traffic.

Note

Your organization's endpoint browsers do not always have to trust the CA certificate of the Threat Isolation Proxy; for example, when your endpoints communicate indirectly with the Threat Isolation Proxy through a downstream proxy that intercepts SSL traffic (see section [3.6.2 "Configuring Symantec Threat Isolation with Downstream Proxy Forwarding"](#)). In this case, the endpoint browsers need to trust only the CA of the downstream proxy, while the downstream proxy must trust the CA of the Threat Isolation Proxy.

You have two options for signing the CA certificate of the Symantec Threat Isolation Platform:

- (Recommended) Using an intermediate CA certificate signed by your organization's root CA. Since your endpoint browsers already trust your organization's root CA, they will also trust any certificates signed by its intermediate CA.

- OR -
- Creating a self-signed CA certificate that is not yet trusted by your endpoints. You will have to deploy the self-signed CA certificate on your endpoint browsers as a trusted CA.

Both of these options include the following steps:

1. [Generating the Encrypted Private Key](#)
2. [Signing the CA Certificate File](#)



3. [Transferring Encrypted Private Key and CA Certificate File](#) to the endpoint where the browser will be logged in to the Management console.

Note

For demo purposes, the system provides a signed CA certificate.

3.4.4.1 Prerequisite

The procedure described in the sections below must be performed on a machine that supports OpenSSL. If your machine does not support OpenSSL, perform the Symantec Threat Isolation Platform installation procedure first, and then proceed with the sections below.

3.4.4.2 Generating the Encrypted Private Key

In this step, you create an OpenSSL configuration file called `openssl.config`, and generate a password-protected encrypted private key file located under the path that you specify.

1. On a machine of your choice that supports OpenSSL, create a file called `openssl.config` under a location of your choice that will be used by commands that mention <OpenSSL configuration file>.
2. Copy the text below into the created <OpenSSL configuration file>.

The <OpenSSL configuration file> serves as an abbreviated version of the default OpenSSL configuration file. The information in <OpenSSL configuration file> is sufficient for use in the OpenSSL commands that you will run for signing a CA certificate.

```
distinguished_name = req_distinguished_name[ req_
distinguished_name ]countryName = Country Name (2 letter
code)stateOrProvinceName = State or Province Name[ localityName
= Locality NameorganizationName = Organization NamecommonName
= Common NameemailAddress = Email Address[ ca
]subjectKeyIdentifier = hashauthorityKeyIdentifier =
keyid:always,issuerbasicConstraints = critical,
CA:truekeyUsage = critical, digitalSignature, cRLSign,
keyCertSign[ intermediate_ca ]subjectKeyIdentifier =
hashauthorityKeyIdentifier =
keyid:always,issuerbasicConstraints = critical, CA:true,
pathlen:0keyUsage = critical, digitalSignature, cRLSign,
keyCertSign
```




When you run the OpenSSL commands, you will be prompted for input for the following parameters that are contained in the <OpenSSL configuration file>:

- ◆ `countryName` – The two-letter code for the country in which your Management server is located.
- ◆ `stateOrProvinceName` – The name of the state or province in which your Management server is located.
- ◆ `localityName` – The name of the locality in which your Management server is located.
- ◆ `organizationName` – The name of your organization.
- ◆ `commonName` – The recognized name of your organization. For example, if you work at MyOrganization, you would call it: MyOrganization-CA.

Note

Do NOT use the hostname of the Threat Isolation Proxy as the Common Name.

- ◆ `emailAddress` – the email address for your organization's security official who should receive notifications.

3. To generate the private key file, run:

```
openssl genrsa -aes256 -out <CA certificate key> 4096
```

where <CA certificate key> is the path of the output encrypted private key file.

4. When prompted, specify the pass phrase for the password-protected encrypted private key file.

Note

If you run the above command on the Symantec Threat Isolation Platform and get the error "unable to write 'random state'", run: `sudo rm ~/.rnd` and then run the OpenSSL command again.

The output of this step:

- ◆ The <OpenSSL configuration file> abbreviated configuration file, located under the location that will be used by commands that mention <OpenSSL configuration file>
- ◆ The password-protected encrypted private key file, located under the path specified in <CA certificate key>



3.4.4.3 Signing the CA Certificate File

In this step, you sign a CA certificate file that will be trusted by all endpoints. The CA certificate file can be one of the following:

- An intermediate CA certificate signed by your organizational root CA (recommended)
- OR -
- A self-signed CA certificate

Using an intermediate CA certificate signed by your organizational root CA

It is recommended to use an intermediate CA certificate that is signed by your organizational root CA. If the Threat Isolation Proxy's CA certificate is an intermediate CA certificate signed by your organizational root CA, the endpoint browsers in your organization will automatically trust all server certificates that are signed by it.

Note

You can choose to use an intermediate CA certificate signed by the CA of your downstream proxy (for example, ProxySG) instead of by your organizational root CA.

To create an intermediate CA certificate signed by your organization's root CA for the Threat Isolation Proxy:

1. Create a Certificate Sign Request (CSR) and submit it to your organizational root CA for signing as an intermediate CA certificate.

To create the CSR file, run:

```
openssl req -new -sha256 -config <OpenSSL configuration file>  
-extensions "intermediate_ca" -key <CA certificate key> -out  
<CSR file>
```

where:

- ◆ <CA certificate key> is the path of the encrypted private key file generated in the step [“Generating the Encrypted Private Key”](#)
 - ◆ <OpenSSL configuration file> is the openssl.config file generated in the step [“Generating the Encrypted Private Key”](#)
 - ◆ <CSR file> is the location of the output CSR file
2. When prompted, enter the passphrase for the password-protected encrypted private key file.



3. When prompted, specify the information that will be incorporated into your certificate request.

Note

Do NOT use the hostname of the Threat Isolation Proxy as the Common Name.

4. Send the output CSR file, located under <CSR file>, to the security team that has permission to sign organizational intermediate CA certificates.

The security team will run an equivalent of the following command:

```
openssl x509 -req -days 1024 -in <CSR file> -CA <root CA
certificate file> -CAkey <root private key> -CAcreateserial -
out <intermediate CA certificate file> -sha256 -extfile
<OpenSSL conf file> -extensions "intermediate_ca"
```

where:

- ◆ <root CA certificate file> is the root CA certificate
- ◆ <root private key> is the root CA private key
- ◆ <intermediate CA certificate file> is the location of the output intermediate CA certificate file
- ◆ <OpenSSL configuration file> is the openssl.config file generated in the step [“Generating the Encrypted Private Key”](#)

The team will send the output CA certificate file defined in <intermediate CA certificate file> to you.

Using a self-signed CA certificate

1. To create a self-signed CA certificate, run:

```
openssl req -x509 -new -nodes -days 1024 -sha256 -config
<OpenSSL configuration file> -extensions "ca" -key <CA
certificate key> -out <CA certificate>
```

where:

- ◆ <OpenSSL configuration file> is the openssl.config file generated in the step [“Generating the Encrypted Private Key”](#)
- ◆ <CA certificate key> is the path of the encrypted private key file generated in the step [“Generating the Encrypted Private Key”](#)
- ◆ <CA certificate> is the path of the output self-signed CA certificate file



2. When prompted, enter the passphrase for the password-protected encrypted private key file.

The output of this step (both for the intermediate CA signed by your organizational root CA and the self-signed CA certificate), is:

- The password-protected encrypted private key file generated in the step [“Generating the Encrypted Private Key”](#)
- The CA certificate file

Note

In topologies where the self-signed CA certificate file must be deployed to all endpoint browsers in your organization, the recommended deployment method for IE and Chrome in Windows is through GPO. Otherwise, or in case of a small number of users, it can be deployed manually. For more information, see section [3.5.11 “Installing the CA Certificate as Trusted Root CA on the Client Side”](#).

3.4.4.4 Transferring Encrypted Private Key and CA Certificate File

In this step, you transfer the encrypted password-protected private key file and the CA certificate file to the endpoint where the browser will be logged in to the Management Console. When you define Symantec Threat Isolation components using the Management UI, you will use these files for the following purposes:

- To associate the CA certificate with your Zone, as described in section [3.5.10 “Associating the CA Certificate with Your Zone”](#), and
- To configure the Zone, as described in section [4.7.2 “Configuring the Zone”](#).

3.5 Installing the Symantec Threat Isolation Platform

3.5.1 Overview

This section describes the steps you must perform to install the Symantec Threat Isolation Platform system. You can install the Symantec Threat Isolation Platform system in several ways:

- **As a distributed system**, where Symantec Threat Isolation components such as the PDP, Threat Isolation Proxies, and Threat Isolation Engines (TIEs) are distributed over multiple physical or virtual machines (VMs) and networks. Instructions in the following sub-sections describe the installation of a distributed system.
- **As an all-in-one solution**, where all components reside on a single physical machine. This installation is used primarily for demo and proof-of-concept systems.

**IMPORTANT!**

Install your Symantec Threat Isolation Platform in the following order.

STEP 1: Prepare each machine to run the Symantec Threat Isolation Platform components.

This step involves:

1. [Preparing the Symantec Threat Isolation Platform Machine](#)
2. [Downloading the ISO File and Verifying the MD5 Signature](#)
3. [Configuring the Machine for Loading the ISO File](#)
4. [Booting the Machine and Starting Installation](#)

STEP 2: Set up the Management Gateway.

This step involves:

1. [Initializing the Symantec Threat Isolation Platform](#)
2. [Initializing the Management Gateway](#)
3. [Defining the Management Gateway](#)

Note

All steps prior to defining the Management Gateway, using the First Time Wizard, must be performed for *each machine* that you install.

STEP 3: Use the Management interface to define additional Gateways.

This step involves:

1. [Defining Symantec Threat Isolation Components](#)
2. [Deciding Where the PDP Will Reside](#)
3. [Defining a Threat Isolation Gateway](#)
4. [Initializing Gateways](#)

STEP 4: Complete the settings and push them to the Gateways.

This step involves:

1. [Associating the CA Certificate with Your Zone](#)
2. [Pushing Settings to the Gateways](#)

**STEP 5: Deploy the CA certificate on the clients.**

This step involves:

- [Installing the CA Certificate as Trusted Root CA on the Client Side](#)

3.5.2 Preparing the Symantec Threat Isolation Platform Machine

Prepare the machine where the Symantec Threat Isolation Platform will be installed:

- Physical appliance – Make sure the machine meets the minimum resource requirements for running Symantec Threat Isolation. For more information, see section [3.1 "System Requirements"](#).
- Virtual Machine (VM) – Create a VM that meets the minimum resource requirements for running Symantec Threat Isolation. For more information, see section [3.1 "System Requirements"](#).

Important: Since Symantec Threat Isolation is a real-time system, the VM must never be in a situation where the minimum resources for running the system are not available to it. To prevent this situation, do the following:

- ◆ Configure the host machine to always reserve the required minimum hardware resources (CPU and memory) for the VM.
- ◆ It is good practice to schedule tasks that require high consumption of host machine resources, such as backup procedures of guest machines, during off-peak hours.

3.5.3 Downloading the ISO File and Verifying the MD5 Signature

1. Access the file needed for installing your Symantec Threat Isolation system from <https://support.symantec.com>.
2. Go to Downloads > Network Protection (Blue Coat) Downloads.
3. In the Download Central Home page, select Isolation in the My Products column, then select Isolation-VA under Product Lines.
4. In the Product Information page, Product Versions tab, select the product version described in this guide.
5. In the Product Download page, Files tab, select the ISO file checkbox and then expand its download information.

The HTTPS Download file, MD5 Signature and additional information are displayed.



4 Files	
	File Size
HTTPS Download	2.7 GB
fireglass_install_1.9.54+223.iso	
File Type	N/A
Operating System	N/A
Product Description	N/A
MD5 Signature	abd2bd262cf16eac4b7ad33e8755c222
	7 MB
	6.9 MB
	392.8 KB

6. Download the ISO file.
7. Verify the MD5 signature of the downloaded ISO file against the MD5 signature in the Product Download window.

For example, for Linux, run:

```
md5sum <path to the downloaded file>
```

Compare the signature calculated for the downloaded ISO file with the value listed in MD5 Signature in step 5. They should match.

Note

If you prefer to use an OVA file, contact Symantec Threat Isolation technical support.

3.5.4 Configuring the Machine for Loading the ISO File

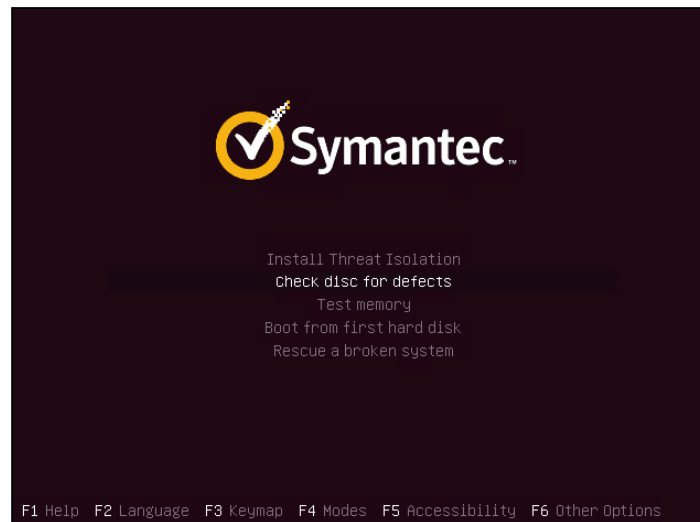
Configure the machine as follows:

- Physical appliance – Create a bootable media device (such as a DVD or USB flash drive) that contains the ISO file, or configure the appliance to load the ISO file from the network.
- Virtual Machine (VM) – Edit the VM settings so that its virtual CD/DVD device is configured to use the ISO file.

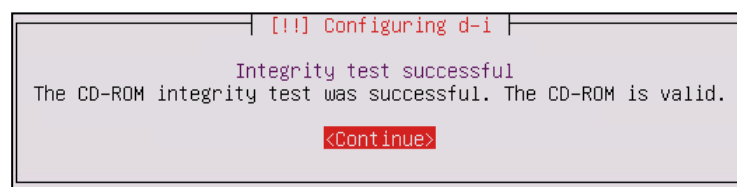
3.5.5 Booting the Machine and Starting Installation

Once the machine has been configured to boot from the ISO file, boot it to start Symantec Threat Isolation Platform installation:

1. When the installation starts, choose the second option presented on the screen:
 - ◆ Check disc for defects

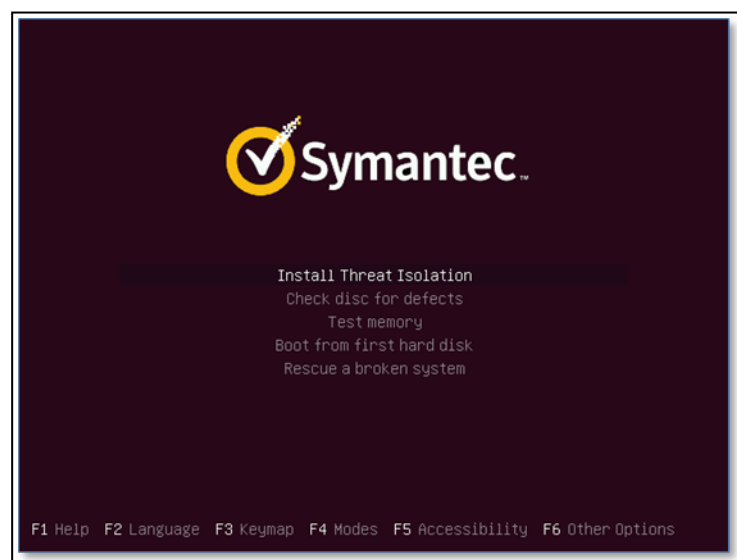


2. When checking the disc is completed successfully, click Continue.



3. Choose the first option presented on the screen:

- ◆ Install Threat Isolation



4. At the end of the installation, the system reboots automatically.



5. An automatic bootstrap process occurs before you can log in to the system. Wait for a prompt and for the Login screen to appear on the machine's console.

3.5.5.1 Changing the Operating System Password

1. Log in to the installed machine via the machine's console, using the following default credentials:

- ◆ Username: `fireglass`

- ◆ Password: `fireglass`

2. At the command line, go to `root` and type the following:

```
sudo passwd fireglass
```

3. Enter your new password.
4. Enter your new password a second time.

When the password is changed successfully, the following message is displayed:

```
password updated successfully
```

3.5.6 Initializing the Symantec Threat Isolation Platform

3.5.6.1 Initializing the Symantec Threat Isolation Platform

1. Log in to the Threat Isolation Gateway machine console.
2. Run the following command:

```
sudo fgcli setup
```

The Network Configuration Wizard starts.
3. Follow the instructions of the wizard to perform Initial Setup.
4. The system re-initializes, and the following message is displayed:

```
Done
```

3.5.6.2 Initializing the Management Gateway

Initializing the Management Gateway presumes that you have initialized the Symantec Threat Isolation Platform, as explained in section [3.5.6.1 "Initializing the Symantec Threat Isolation Platform"](#).



The following prompt appears:

```
Is this the Management gateway? [y/N]
```

Type `y`.

Do the following:

1. Log in to the Admin Terminal and make sure it has network access to the current machine.

For more information, see the relevant topology diagram under section [2.6 "Deployment Topologies"](#).

2. Define the Management Gateway, as explained in section [3.5.7 "Defining the Management Gateway"](#).

3.5.7 Defining the Management Gateway

You define the Management Gateway using the First Time Wizard. This utility enables you to configure the following:

- The Management host and time zone settings
- Administrator credentials
- SSL termination, if used
- Active Directory settings, if used


1. Open the Symantec Threat Isolation Management UI.

From your web browser, open the URL:


```
https://<management host or IP>:9000
```


The login page appears.




 **Symantec™**

Please enter your credentials:

 Username

 Password



2. Enter the following default credentials:
Username: admin
Password: admin
3. Click the arrow to log in.



The License Agreement window appears.

License Agreement

Please read and accept the following license agreement:

SYMANTEC SOFTWARE LICENSE AGREEMENT

SYMANTEC CORPORATION AND/OR ITS AFFILIATES ("SYMANTEC") SPECIFIED IN THE ENTITLEMENT CONFIRMATION IS WILLING TO LICENSE THE LICENSED SOFTWARE TO YOU AS THE INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE LICENSED SOFTWARE (REFERENCED BELOW AS "YOU" OR "YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS AND CONDITIONS OF THIS SYMANTEC SOFTWARE LICENSE AGREEMENT AND THE PRODUCT USE RIGHTS SUPPLEMENT (AS DEFINED BELOW) (COLLECTIVELY, THE "LICENSE AGREEMENT"). READ THE LICENSE AGREEMENT CAREFULLY BEFORE USING THE LICENSED SOFTWARE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY DOWNLOADING, INSTALLING, COPYING, CLICKING THE "I AGREE" OR "YES" BUTTON, OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, OR USING THE LICENSED SOFTWARE, YOU AGREE TO THE TERMS AND CONDITIONS OF THE LICENSE AGREEMENT. IF YOU DO NOT AGREE TO THE LICENSE AGREEMENT, CLICK THE "I DO NOT AGREE" OR "NO" BUTTON OR OTHERWISE INDICATE REFUSAL AND CEASE ANY AND ALL USE OF THE LICENSED SOFTWARE.

1. DEFINITIONS. Unless otherwise defined in this License Agreement, capitalized terms will have the meaning given below and such capitalized terms may be used in the singular or in the plural, as the context requires.

"**Collected Data**" means certain information which Symantec may collect, retain, process, disclose and use in connection with Your use of the Licensed Software, or Your devices or systems with which the Licensed Software operates, and may include, but is not limited to, Personal Information about You, about Your employees, agents or contractors acting on Your behalf.

"**Content Updates**" means content, which may be provided from time to time, used by certain Symantec products and/or services to maintain the efficacy of the product, including but not limited to: updated anti-spyware definitions for anti-spyware products; updated antispam rules for antispam products; updated virus definitions for antivirus and crimeware products; updated URL lists for content filtering and antiphishing products; updated firewall rules for firewall products; updated intrusion detection data for intrusion detection products; updated lists of authenticated web pages for website authentication products; updated policy compliance rules for policy compliance products; and updated vulnerability signatures for vulnerability assessment products. Content Updates may include content produced by the Licensed Software based on Your use of the Licensed Software. "Documentation" means the user documentation, user manual, and release notes provided for the Licensed Software. Documentation may be delivered in a text file, printed form or published on a product Web page.

"**Entitlement Confirmation**" or "**License Instrument**" means one or more of the following applicable documents which further defines Your license rights to the Licensed Software and Your access to Maintenance, including, but not limited to: a Symantec license or maintenance certificate or a similar confirmation document issued by Symantec; or a written agreement between You and Symantec; or validation through an entitlement portal, or an authorized Symantec email confirmation, or an order confirmation receipt, that accompanies, precedes or follows this License Agreement.

"**Licensed Software**" means the Symantec software product, in object code form, accompanying this License Agreement, including

☐ I accept the terms of this agreement

Page 1 out of 7

BACK NEXT CLOSE

4. Read the terms of the license agreement and check the checkbox to accept them, then click Next.

The Initial Settings window appears.



The image shows a web-based configuration window titled "Initial Settings". It is divided into two main sections: "Management settings" and "Local time". Under "Management settings", there is a label "Management Host Name" followed by a text input field containing the placeholder "<your management host>". Under "Local time", there is a label "Timezone" followed by a dropdown menu with the text "Select a time zone...". Below these sections, there are two checkboxes. The first checkbox is checked and is labeled "Enable SSL termination". The second checkbox is unchecked and is labeled "I am configuring this appliance offline". At the bottom of the window, there is a footer area that says "Page 2 out of 7" on the left and three buttons labeled "BACK", "NEXT", and "CLOSE" on the right. The "NEXT" button is highlighted in blue.

5. Fill in the following fields:
 - ◆ Management Host Name - This is the DNS name for the Management machine. Specify its public DNS host name.
 - ◆ Timezone - Time zone for the geographic location of your Management machine.
 - ◆ Enable SSL termination - Select if your country allows SSL termination.
 - ◆ I am configuring this appliance offline - Select if you are performing the configuration offline (not connected to the network). If you are performing the configuration offline, any processes or AD configuration will take effect the next time this machine is connected to the network.
6. Click Next.

The Authentication Settings window appears.



Authentication Settings

Administrator account

Username Username

Password Password Strength: None

Retype Password Password

Email Email

Page 3 out of 7

BACK NEXT CLOSE

7. Fill in the following fields:
 - ◆ Username - For added security, type a username to replace the "admin" default
 - ◆ Password - Type a password
 - ◆ Retype Password - Type the above password a second time

Note

You can reset this password later from the Management console. You can also reset a Management user password from outside of the Management console by running fgcli. For instructions, see section [3.11.3 "Resetting a Management User Password"](#).

- ◆ Email - Email address for receiving notifications
8. Click Next.

The Active Directory window appears.



9. Select Active Directory and define the settings as explained in section [4.5.2 "Defining Active Directory Settings"](#).

Note

You can choose to specify the Active Directory settings later, as explained in section [4.5.2 "Defining Active Directory Settings"](#). In this case, click Next to proceed to the next step.

10. Click Next.

The Product Registration window appears.



The screenshot shows the 'Product Registration' window. It has two main sections: 'Registration Information' and 'License Information'. Under 'Registration Information', there are two radio buttons: 'Online Registration' (selected) and 'Offline Registration'. The 'Online Registration' section has three input fields: 'User Name' (placeholder: Symantec NPLP User Name), 'Password' (placeholder: Symantec NPLP Password), and 'Serial Number' (placeholder: Management VA Serial Number). There is a 'REGISTER' button next to the 'Serial Number' field. The 'Offline Registration' section has a 'License File' input field and a 'REGISTER...' button. Below these is the 'License Information' section, which contains a blue button that says 'Register a license to view information' and a checkbox labeled 'I'll register later'. At the bottom of the window, it says 'Page 5 out of 7' and has 'BACK' and 'NEXT' buttons.

11. Register your licensed components.

Notes

- You can choose to register your licensed components later. In this case, select the I'll register later checkbox, and click Next to proceed to the next step.
- For information about how to register licensed components later, see section [4.20.1 "Registering your Licensed Components"](#).

Prerequisite

In the components registration procedure, several steps must be performed in Symantec's Network Protection Licensing Portal (NPLP).

- ◆ Open the NPLP as follows:
https://services.bluecoat.com/eservice_enu/licensing
- ◆ In the NPLP, retrieve the VA Serial Number:
 - Select Isolation > VA Serial Number Retrieval from the left menu.
 - Specify the Activation Code that Symantec provided by email when the components were purchased, and then click Submit.

The Management VA Serial Number is returned. From this point forward, this serial number is the Symantec Identity for your device.



Registering the licensed components

In the Product Registration window, perform one of the following procedures:

- ◆ Online registration
 - i. Under Registration Information, select Online Registration.
 - ii. Provide the following:
 - Your MySymantec customer login credentials, which you specified when you created a MySymantec Account (as a Getting Started step, described in the Fulfillment Acknowledgment email)
 - The VA Serial Number
 - iii. Click Register.

- ◆ Offline registration

You can choose this option when you are not the person who created the MySymantec Account, or when the endpoint from which the First Time Wizard is launched does not have Internet access.

Prerequisite

From the NPLP, download the license file as follows:

- i. Select Isolation > License Download from the left menu.
- ii. Specify the VA Serial Number and a PassPhrase.

Note

The PassPhrase is used for encrypting the private encrypted certificate, which is part of the license file. It must include at least eight alphabetic and/or numeric characters.

- iii. Click Next, and then download the license file.

Registering Offline

In the Product Registration window, do the following:

- i. Under Registration Information, select Offline Registration.
- ii. Click Register... and then choose the downloaded license file from your file system. The file has the following format: license_<serial_number>.bcl
- iii. In the License File PassPhrase pop-up window, type the PassPhrase you specified in the NPLP (see step ii., above).
- iv. Click OK.

**Note**

Once your licensed components are registered, you can view or modify your current license status. For more information, see section [4.20.1.3 "Viewing Current License Information"](#).

Activating add-ons

If you have subscribed to the additional URL Categorization and/or Risk Levels services, it is recommended to activate these add-ons now.

In the NPLP, do the following:

- a. Select Isolation > Software Add-on Activation from the left menu.
- b. Specify the VA Serial Number and the Activation Code^[1] that Symantec provided by email when you purchased the add-on.
- c. Click Submit.

Note

The STIP needs a few minutes to be updated with the changes you made in the NPLP. When this process is complete, you can start using the add-ons.

When you have completed registering your licensed components in the Product Registration window, click Next.

The Components screen appears.

[1] In the order confirmation email, these add-ons may be referred to as: *BCIS Standard Web Security and Web Applications for SWG and *BCIS Advanced Web Security with Risk Controls and Web Applications for SWG.



Components

Components to activate on this server:

Gateway components

- ☐ Proxy
- ☐ Threat Isolation Engine
- ☒ Policy Distribution Point

Management components

- ☒ Management
- ☒ Report Server

Page 6 out of 6

BACK FINISH

12. If your Management machine will function as a Threat Isolation Gateway and run Gateway components, select the relevant checkboxes. For more information, see section [3.5.8 "Defining Symantec Threat Isolation Components"](#).

Note

A warning appears when you select only the Policy Distribution Point checkbox. For more information, see [3.5.8.1 "Deciding Where the PDP Will Reside"](#).

The Report Server always resides on the Management machine. It is typically enabled from the Components screen, as shown above.

Note

You can choose to enable the Report Server later, as follows.

On the Management Server machine that activates the Report Server component, run:

```
sudo fgcli service install report-server
```

13. Click Finish.

The Login screen appears.

14. Log in to start using the Management console.

3.5.8 Defining Symantec Threat Isolation Components

From the Symantec Threat Isolation Management console, define the following components:



■ Threat Isolation Gateways

To define Gateways, follow the instructions in section [4.7.7 "Defining a Threat Isolation Gateway"](#).

For each Gateway, define its components:

- ◆ Threat Isolation Engine (TIE) – To define TIEs, follow the instructions in section [4.7.9 "Defining Threat Isolation Engines \(TIEs\)"](#).
- ◆ Threat Isolation Proxy – To define Threat Isolation Proxies, follow the instructions in section [4.7.10 "Defining Threat Isolation Proxies"](#).

Note

If there is a next hop proxy/server for the Gateway (Threat Isolation Engine (TIE)/Threat Isolation Proxy) that performs SSL termination, contact Symantec Threat Isolation technical support for assistance.

■ Policy Distribution Point (PDP)

- ◆ In on-premises deployments, the PDP typically resides on the TIE Gateway (in the DMZ). By default, the PDP will reside on the first TIE that you register. For more information, see section [3.5.8.1 "Deciding Where the PDP Will Reside"](#).
- ◆ In cloud deployments, the PDP resides on the Management component.

3.5.8.1 Deciding Where the PDP Will Reside

The following points should be considered when deciding where the Policy Distribution Point (PDP) will reside:

- The PDP relays control messages between gateways. The Management server, Threat Isolation Proxy and Threat Isolation Engine (TIE) Gateways must all have network access to the PDP (mandatory). In on-premises deployments, it is recommended that the PDP should reside on the TIE Gateway. For more information, see section [2.4 "Platform Components"](#).
- Once the Gateways are interconnected through the PDP, the following takes place above this network:
 - ◆ The Management server distributes the policy to all Gateways through the PDP.
 - ◆ The Gateways synchronize live authorization information through the PDP, allowing TIEs to determine Active Directory group assignments without having direct access to the AD server.



- If one or more Gateways cannot access the Management machine, it is not recommended to locate the PDP on the Management server. However, if the Management server and your Gateways reside on the same network, it is recommended to locate the PDP on the Management server.

3.5.9 Initializing Gateways

Note

This section assumes that you have already created a Threat Isolation Gateway object.

1. Log in to the Gateway machine through its serial console.
2. Run the following command:

```
sudo fgcli setup
```

The Network Configuration Wizard starts.

Note

On a Threat Isolation Engine (TIE) machine, make sure the domain of its FQDN is different than the domain of the organization. For more information, see section [3.4.3.1 "TIE Public DNS Name Considerations"](#).

3. Follow the instructions in the wizard.
4. When the following prompt appears:

```
Is this the Management gateway? [y/N]
```

Type N.

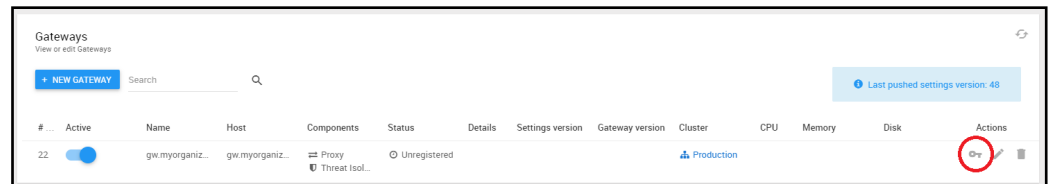
```
Is this the Management gateway? [y/N] n
Gateway is ready for registration.
Copy the fgcli register command from the dialog received when the gateway was created.
If the dialog is not open, open the browser, go to the Gateways page and click the key icon for this
gateway, then copy the register command.
Open an SSH connection from a different PC to the current machine and paste the command into the ter
minal.
```

When the system has reinitialized, the Gateway is ready for registration.



Registering the Gateway

1. Supply the registration command that was generated in the Management user interface, in one of the following ways:
 - ◆ Copy the registration command from the New Gateway Registration dialog that was displayed when the Gateway was created. For more information, see section [4.7.7 "Defining a Threat Isolation Gateway"](#).
 - ◆ If the dialog is not open already, open the browser, go to the Gateways window in the Management user interface. Under Actions, click the key icon for this Gateway (note that the key icon is enabled only when the Gateway is Unregistered). Copy the registration command from the dialog.

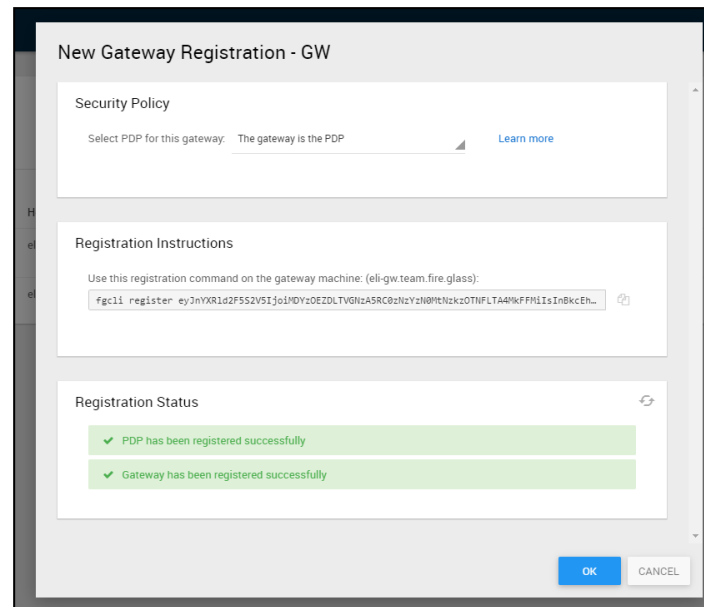


2. Open an SSH connection from the Admin Terminal to the current machine and paste the command into the terminal.
3. Run the command.

When the process is completed, you should see the following:

```
fireglass@ubuntu:~$ fgcli register eyJnYXRld2F5S2V5Ijo1MDYzOEZDLTVGNzA5RC0zNzYzN0MtNzkzOTNFLTAA4MkFFMlIsInBkcEhvc3Q1OjJlbGktZ3cudGVhbSSmaXJLLmd  
3MC00UZF00E1fQ==  
Validating Registration Data [OK]  
Registering PDP [OK]  
Verifying Connectivity to PDP [OK]  
Registering Gateway [OK]  
Configuring Gateway [OK]  
fireglass@ubuntu:~$
```

4. Return to the New Gateway Registration dialog.
5. Under Registration Status, verify that the Gateway (and the PDP, when relevant) were registered successfully.

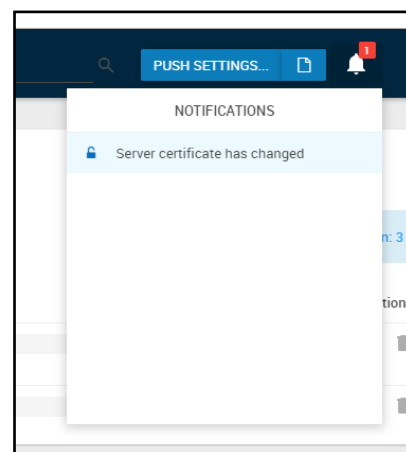


6. Click OK.

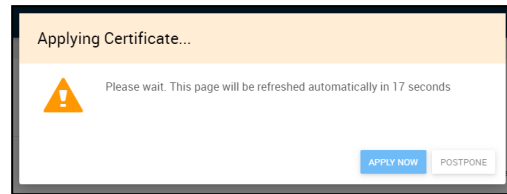
7. Push settings.

The Push Settings button is available from any location in the UI and always appears on the right-hand side of the top bar. For more information, see section [4.7.6 "Pushing Settings"](#).

8. Click the bell icon, and then click the “Server Certificate has changed” notification in the Notifications pop-up.



9. In the Server Certificate Has Changed dialog, click Apply Now.



10. While the Applying Certificate dialog is displayed, wait until the page is refreshed.

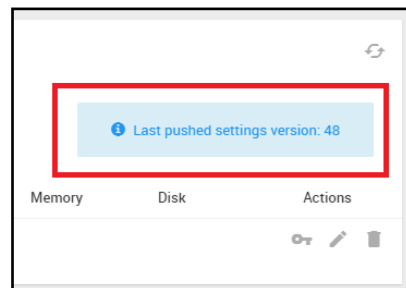
3.5.9.1 Checking Gateway Registrations

- When a Threat Isolation Gateway is created, its status in the Status column of the Gateways page is "Unregistered".



Following initialization, check the Gateway's status in the Status column again and make sure it is now "OK" (meaning, registered).

- Make sure the Last Pushed Settings version (displayed in the upper right-hand corner of the Gateways page) is the same as the latest version listed in the Settings version column for each individual Gateway.



3.5.10 Associating the CA Certificate with Your Zone

This section assumes that you have already signed a CA certificate for the Symantec Threat Isolation Platform by performing all of the steps explained in section [3.4.4 "Signing the CA Certificate"](#). For information about zones, see section [4.7 "Defining Zones, Gateways, and Associated Components"](#).



Symantec Threat Isolation will use the CA certificate for two different purposes:

- To sign the server certificates of HTTPS websites, when Symantec Threat Isolation acts as man in the middle (MITM)
- To sign the server certificates for all gateways (for WebSocket)

As the CA certificate for your Zone, you can choose to use a custom CA certificate that was imported into the Symantec Threat Isolation system (good practice), or the default CA certificate that Symantec Threat Isolation supplies out of the box (recommended only for demo purposes).

To associate the CA certificate with your Zone:

1. In the Management UI, go to:
`System Configuration → Zones → <your zone> → Edit`
2. Select the System CA object to be associated with your Zone. If you have not yet created the System CA object, add it now, and then select it. (For more information, see section [4.8.3 "Adding a System Certificate"](#).)

Note

- It is good practice to have a password-protected CA private key. In this case, you must supply the password to be able to import the key.
- For a description of all Zone parameters, see section [4.7.2 "Configuring the Zone"](#).

3. Click Update to save your changes and close the Update Zone window.
4. Push settings.

3.5.11 Installing the CA Certificate as Trusted Root CA on the Client Side

The CA certificate must be installed as a trusted root certification authority in the endpoint browsers.

Note

This installation is required for all topologies, except the Symantec Threat Isolation as a Web Application Isolation Gateway Mode topology.

3.5.11.1 Deploying the CA Certificate File to the End Users

You can deploy the CA certificate in one of the following ways:

- (Recommended) Through GPO. See instructions at:
<https://technet.microsoft.com/en-us/library/cc738131%28v=ws.10%29.aspx>

**Note**

GPO does not control Firefox browsers.

- (Small number of end users) By sending the CA certificate file to all end users, together with instructions for installation in their browsers, as described in sections [3.5.11.2 "Installing the CA Certificate in Windows Browsers"](#) (for IE and Chrome) and [3.5.11.3 "Installing the CA Certificate in a Firefox Browser"](#) (for Firefox).

3.5.11.2 Installing the CA Certificate in Windows Browsers

Note

The instructions in this section are relevant to Internet Explorer and Chrome browsers. For installing the CA certificate in a Firefox browser, see section [3.5.11.3 "Installing the CA Certificate in a Firefox Browser"](#). For instructions relevant to Mac machines, see section [3.5.11.4 "Installing the CA Certificate on a Mac Machine"](#).

1. Copy the CA certificate that you have defined in section [3.4.4 "Signing the CA Certificate"](#) so that it is accessible from the endpoint machine.

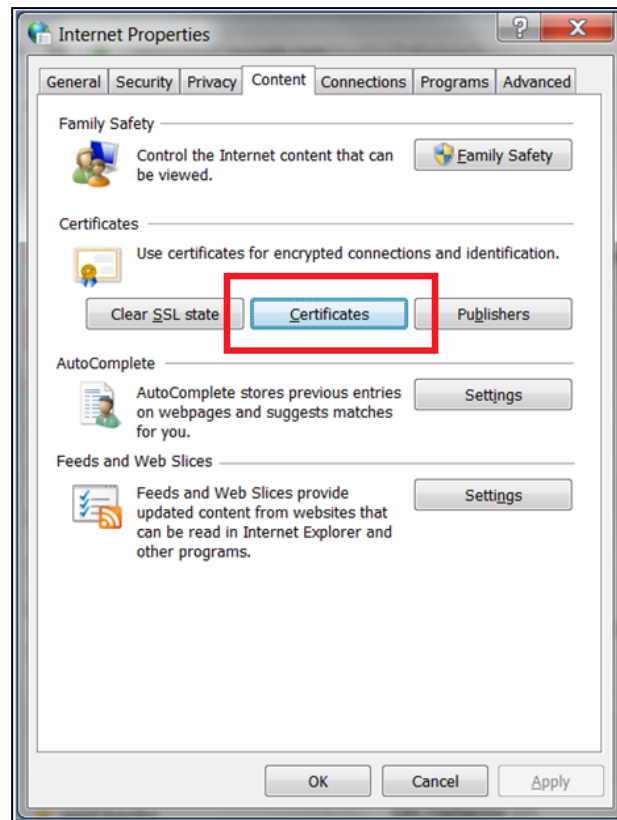
WARNING!

Make sure you do not send the CA key file instead of the CA certificate file by mistake.

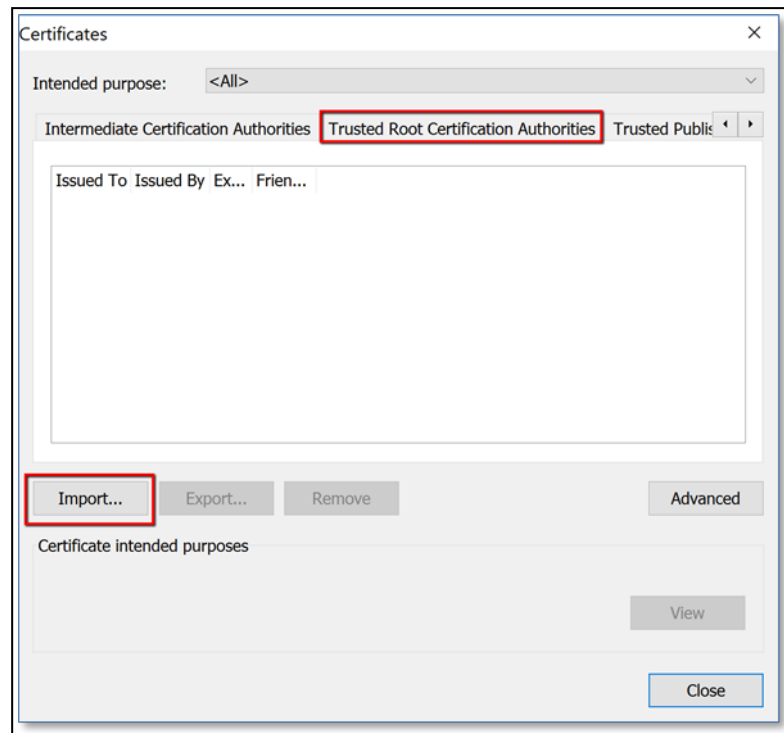
2. In the endpoint browser, go to:
Start -> Settings -> Network & Internet -> Network and Sharing Center
3. Click Internet Options.
4. On the Content tab, click Certificates.



3 Installing the Symantec Threat Isolation Platform

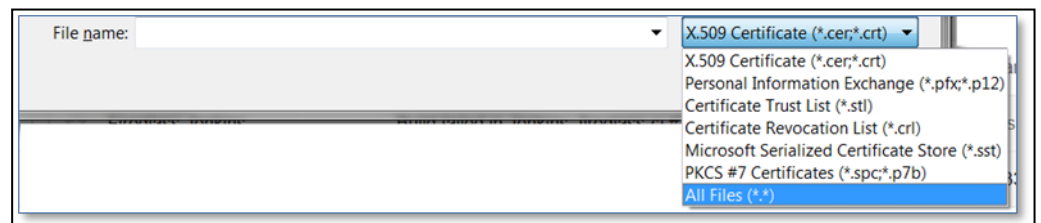


5. On the Trusted Root Certification Authorities tab, click Import.

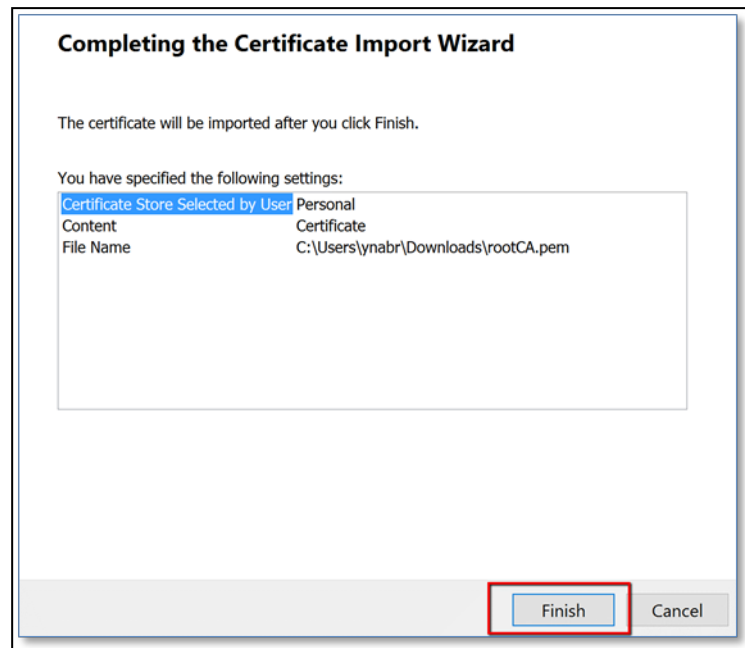


The Certificate Import Wizard opens.

6. Click Next, then click Browse.
7. Open the file type drop-down list, scroll all the way to the bottom of the list, and choose All Files.

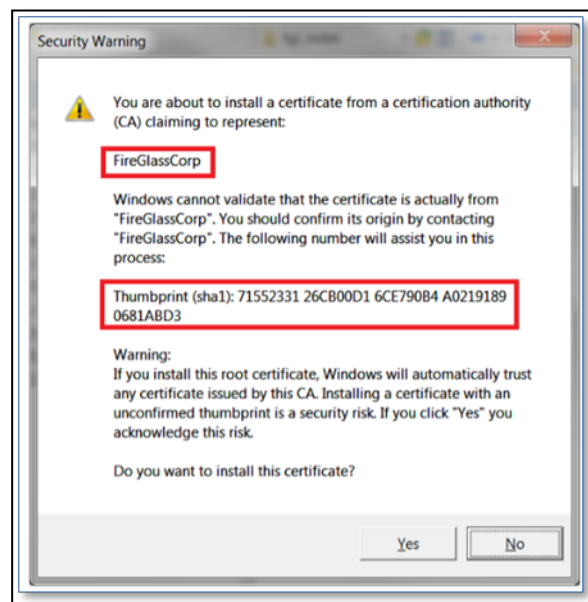


8. Select the CA certificate path.
9. Click Open, then click Next.
10. Select Place all certificates in the following store, then click Browse and choose the option Trusted Root Certification Authorities.
11. Click Next.



12. Click Finish.

A Security Warning appears. Note that the information highlighted in the screenshot below is defined per customer. Therefore, it appears differently for each customer.



13. Click Yes.



The Certificate Import Wizard screen opens, indicating that the import was successful.

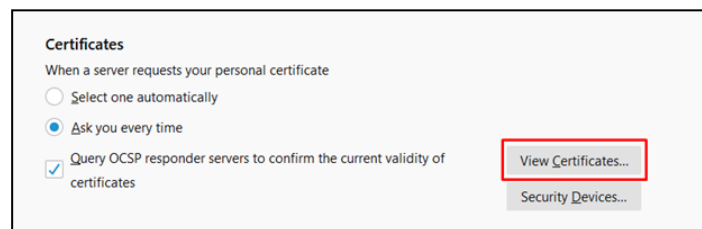
14. Click OK.

3.5.11.3 Installing the CA Certificate in a Firefox Browser

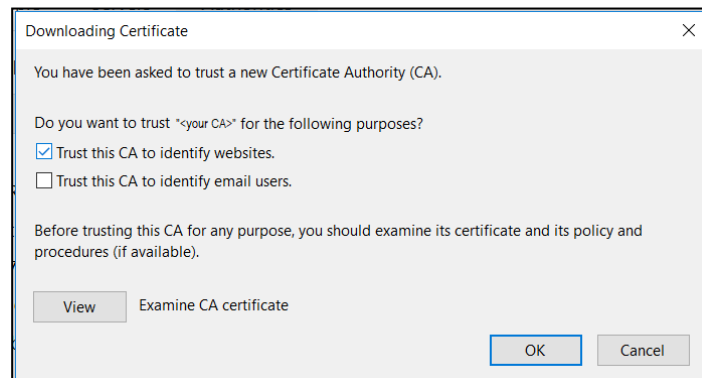
Note

GPO does not deploy for Firefox browsers.

1. In the Firefox browser, open Options.
2. Click the Privacy & Security tab.
3. Under Certificates, click View Certificates.



4. Display the Authorities tab and click Import.
5. Choose the CA certificate file.
6. In the following pop-up, select the first checkbox:



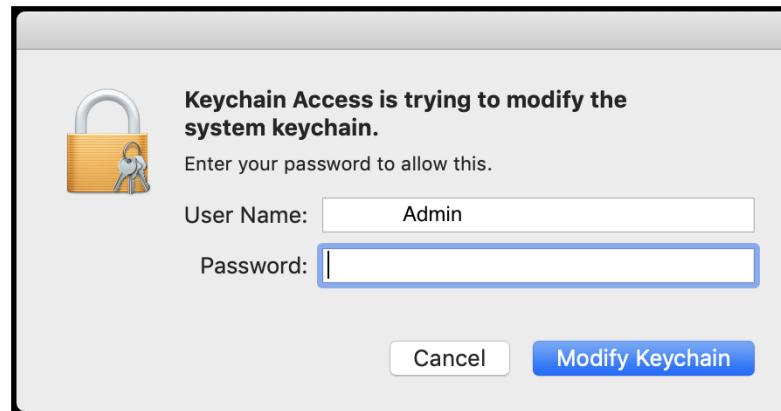
7. Click OK.
8. Click OK to complete the procedure.

3.5.11.4 Installing the CA Certificate on a Mac Machine

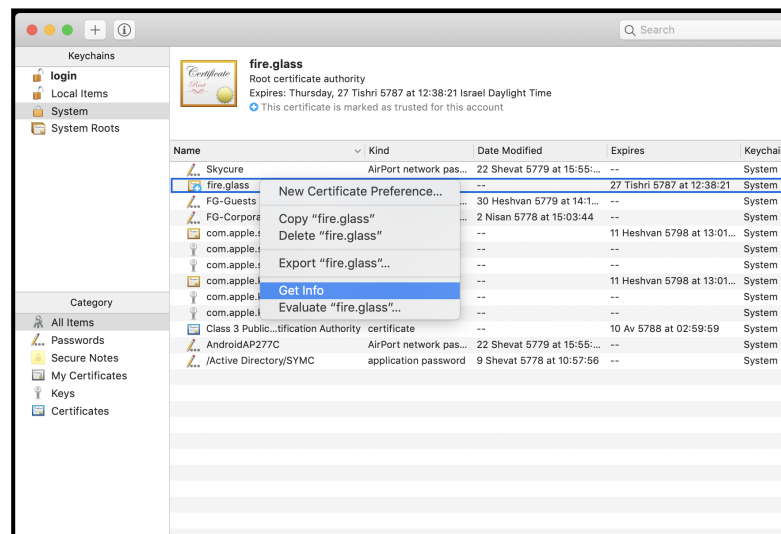
1. On a Mac endpoint machine, double-click the CA certificate file.



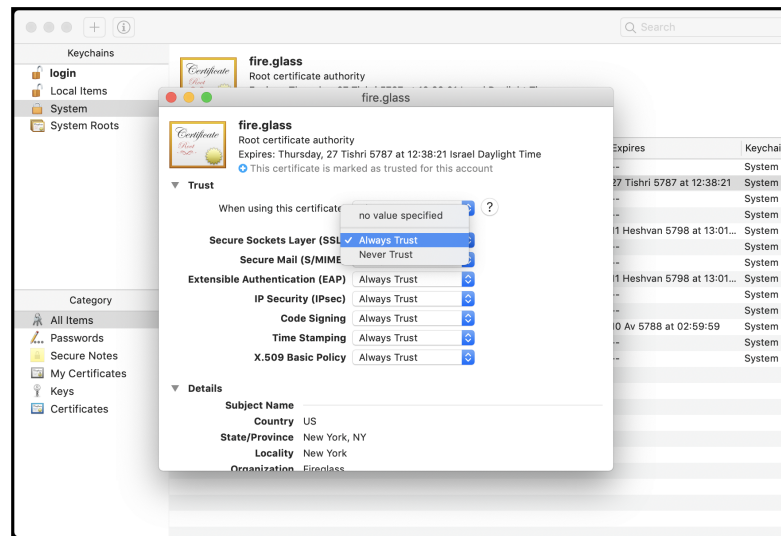
2. Enter the administrator password, and then click Modify Keychain.



3. Go to "spotlight" (the search icon in the top right corner), search for Keychain Access, and then select Keychain Access from the search results.
4. Under System, highlight the certificate that you added.
5. Right-click and choose Get Info from the context menu.



6. Expand Trust to display the trust policies for the certificate.
7. Under Secure Sockets Layers (SSL), select Always Trust.



3.5.12 Verifying the Trusted Root CA in the Endpoint Browser

It is important to make sure the CA certificate was installed properly as a trusted root Certification Authority in each browser type used in your organization.

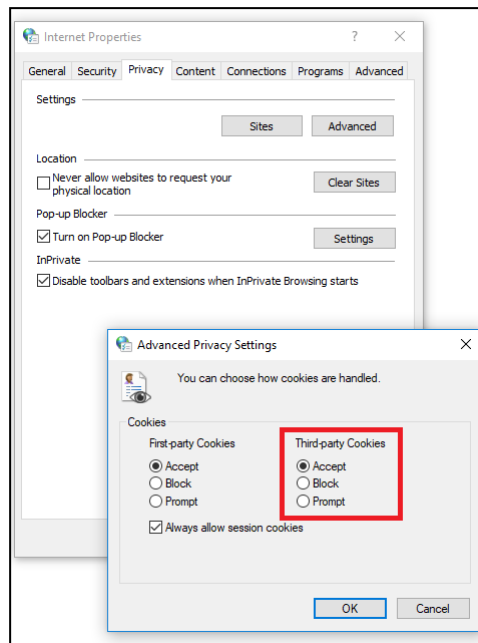
1. Go to Internet Options and click the Content tab.
2. Under Certificates, verify that the CA certificate is listed as a trusted root Certification Authority.

3.5.13 Making Sure Third-Party Cookies Are Accepted

In every isolated website, the Symantec Threat Isolation block page contains subresources that are directed to the Threat Isolation Proxy/Threat Isolation Engine (TIE) Gateways. Symantec Threat Isolation might need to set cookies directed to a third-party host (for example, the TIE) to be able to maintain a state. For this purpose, accepting third-party cookies must be enabled in the endpoint browser settings. Verify this, as follows.

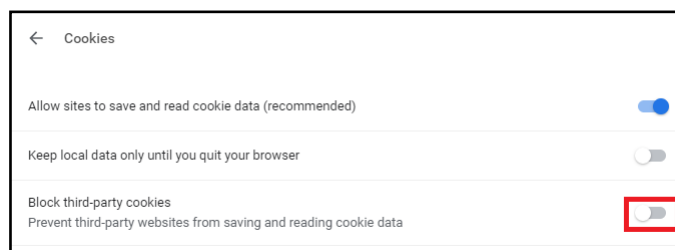
In Internet Explorer:

1. Go to Tools > Internet Options.
2. In the Internet Properties dialog, open the Privacy tab and click Advanced.
3. Under Third-party Cookies, make sure Accept is selected (default).



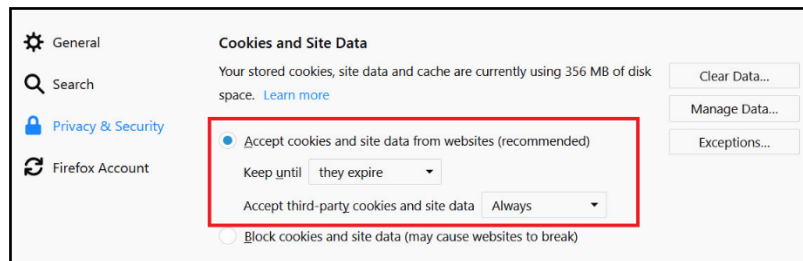
In Chrome:

1. Go to Settings > Advanced.
2. In Privacy and security, click Content settings and then Cookies.
3. Make sure Block third-party cookies is disabled (default).



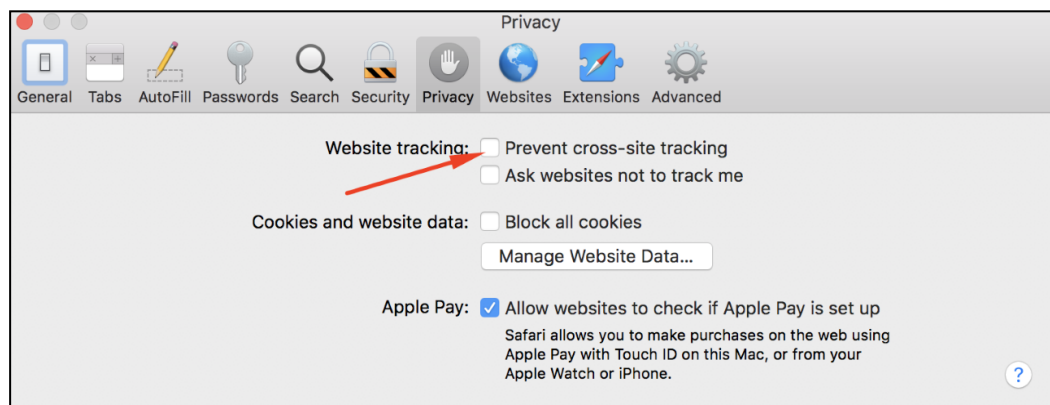
In Firefox:

1. Go to Options > Privacy & Security.
2. Under Cookies and Site Data, make sure of the following:
 - ◆ Accept cookies and site data from websites (recommended) is selected.
 - ◆ Accept third-party cookies and site data is set to Always.



In Safari:

1. Go to Preferences > Privacy.
2. In Website tracking, deselect Prevent cross-site tracking.



3.6 Configuring Your Deployment Topology

When you have completed the Symantec Threat Isolation Platform installation procedure, described in section [3.5 "Installing the Symantec Threat Isolation Platform"](#), you need to perform the custom configuration for your deployment topology.

For instructions, refer to the section relevant to your specific topology:

- Symantec Threat Isolation Explicit Proxy topology – section [3.6.1 "Configuring the Symantec Threat Isolation Explicit Proxy Topology"](#)
- Symantec Threat Isolation with Downstream Proxy Forwarding topology – section [3.6.2 "Configuring Symantec Threat Isolation with Downstream Proxy Forwarding"](#)
- Symantec Threat Isolation with Block Page Integration topology – section [3.6.3 "Configuring Symantec Threat Isolation with Block Page Integration"](#)
- Symantec Email Threat Isolation topology – section [3.6.4 "Configuring Symantec Email Threat Isolation"](#)



- Symantec Threat Isolation as Web Application Isolation Gateway Mode topology – section [3.6.5 "Configuring Symantec Threat Isolation as Web Application Isolation Gateway Mode"](#)

Note

For assistance with configuring your deployment topology, contact Symantec Threat Isolation technical support.

3.6.1 Configuring the Symantec Threat Isolation Explicit Proxy Topology

Once you have installed the Symantec Threat Isolation Platform, you need to configure the Explicit Proxy deployment topology. In this topology, all components belong to the Symantec Threat Isolation Platform, and Symantec Threat Isolation functions as a proxy.

This step involves:

1. [Editing the Proxy Auto-Configuration \(PAC\) File](#), if necessary
2. [Configuring the PAC File in a Single Endpoint Browser](#)
3. [Defining Firewall Rules](#)
4. [Pushing Settings](#) to the Threat Isolation Gateways

3.6.1.1 Editing the Proxy Auto-Configuration (PAC) File

If you have installed the Symantec Threat Isolation Explicit Proxy deployment topology, it might be necessary to edit the Proxy Auto-Configuration (PAC) file. For more information, see section [4.7.2.4 "Updating a Zone's PAC File"](#).

3.6.1.2 Configuring the PAC File in a Single Endpoint Browser

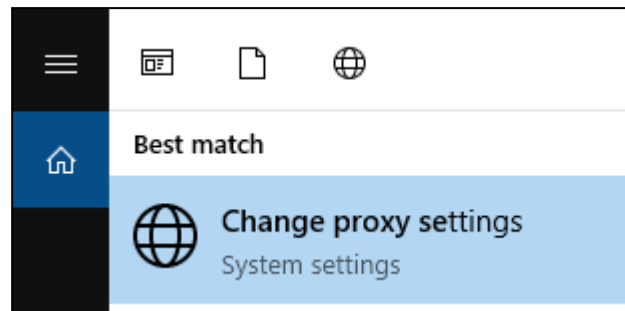
Note

Make sure port 8081 is open on your firewall. For more information, see the Defining Firewall Rules section relevant to your deployment topology.

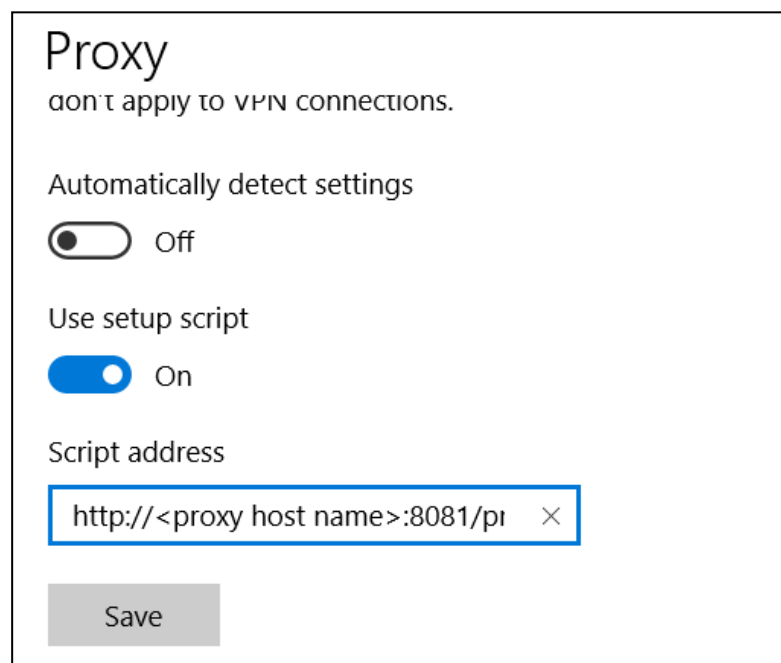
Windows

The procedure below gives an example of how to configure the PAC file manually in a *single* Windows end-user browser. To configure the PAC file in *multiple* Windows end-user browsers, perform the procedure in the Group Policy Object (GPO), described at <http://help.censornetswg.com/web-browser-proxy-settings>.

1. Go to Start.
2. Search for "Change proxy settings" and click the search result:



3. In the Automatic proxy setup section, set the Use setup script switch to On.
4. Fill the Script address field with the following:
`http://<proxy host name>:8081/proxy.pac`



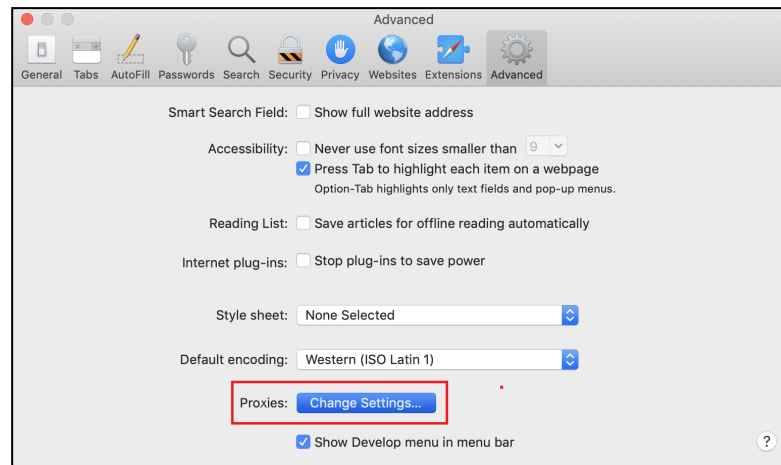
5. Click Save.

Mac

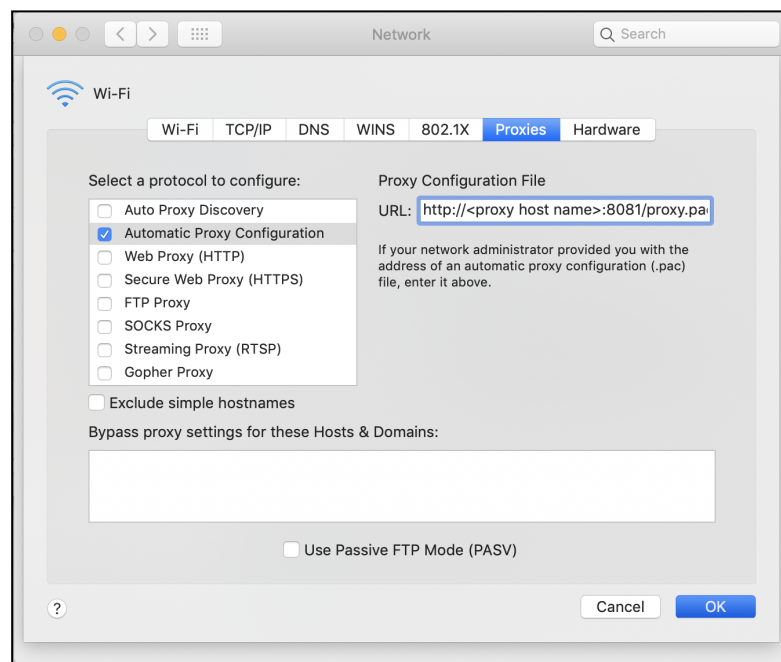
1. Go to Safari > Preferences... and display the Advanced tab.
2. In Proxies, click Change Settings.



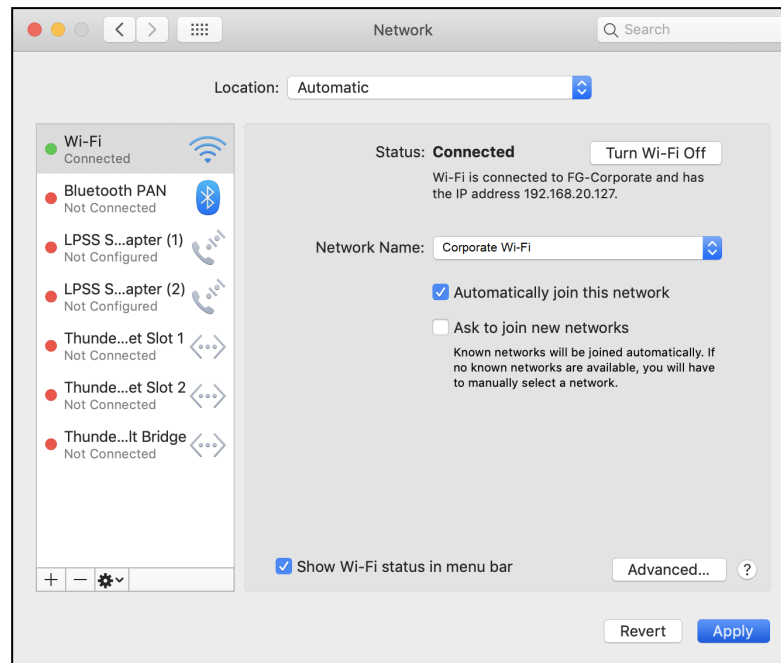
3 Installing the Symantec Threat Isolation Platform



3. Under Select a protocol to configure, select Automatic Proxy Configuration.
4. Under Proxy Configuration File, fill the URL field with the following:
`http://<proxy host name>:8081/proxy.pac`



5. Click OK.
6. In the Network window, click Apply.

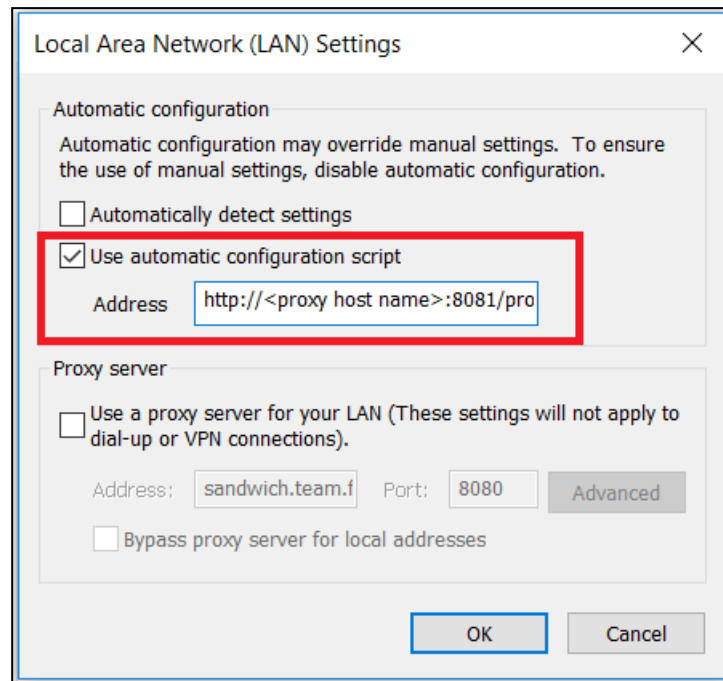


3.6.1.3 Verifying PAC File Configuration in the Endpoint Browser

It is important to verify that the Proxy Auto-Configuration (PAC) file is configured properly in each browser type used in your organization.

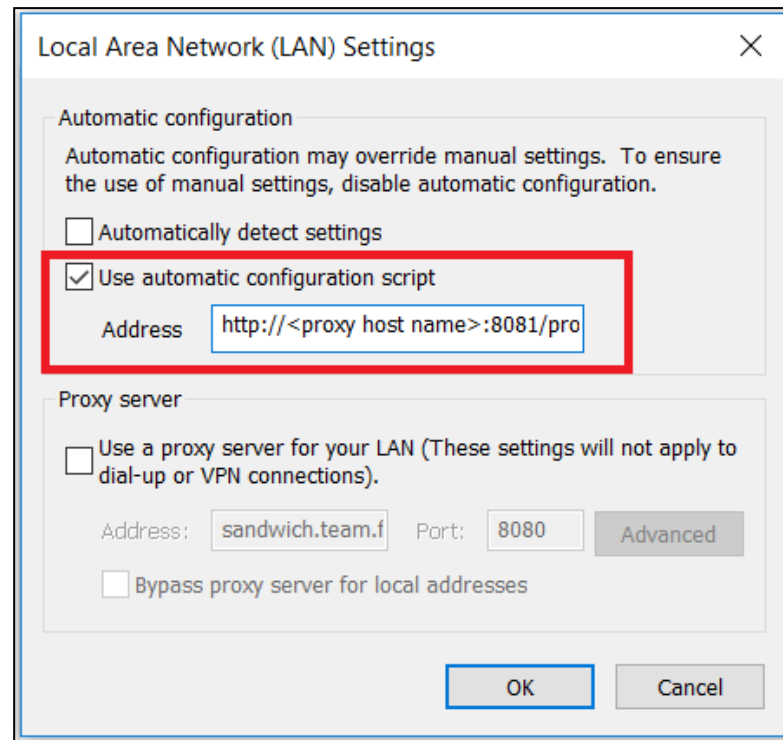
In Internet Explorer:

1. Go to Tools > Internet Options and then click the Connections tab.
2. Click LAN settings.
3. In the Automatic configuration section, make sure of the following:
 - ◆ Use automatic configuration script is selected, and
 - ◆ The Address field is filled with `http://<proxy host name>:8081/proxy.pac`



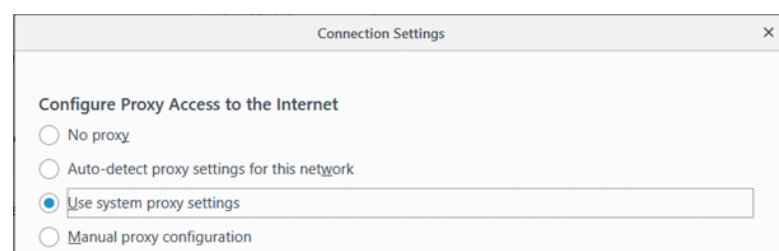
In Chrome:

1. Click Settings.
2. Search for "proxy" and then click Open proxy settings.
3. In the Automatic configuration section, make sure of the following:
 - ◆ Use automatic configuration script is selected, and
 - ◆ The Address field is filled with http://<proxy host name>:8081/proxy.pac



In Firefox:

1. Click Options.
2. Search for “network settings”.
3. Click Settings.
4. In the Configure Proxy Access to the Internet section, make sure Use system proxy settings is selected.



In Edge:

1. Go to Settings > View Advanced Settings > Open Proxy Settings.
2. In the Automatic proxy setup section, make sure of the following:
 - ◆ The Use setup script switch is set to On, and



- ◆ The Script address field is filled with http://<proxy host name>:8081/proxy.pac

Proxy

don't apply to VPN connections.

Automatically detect settings

☐ Off

Use setup script

☒ On

Script address

http://<proxy host name>:8081/pa

Save

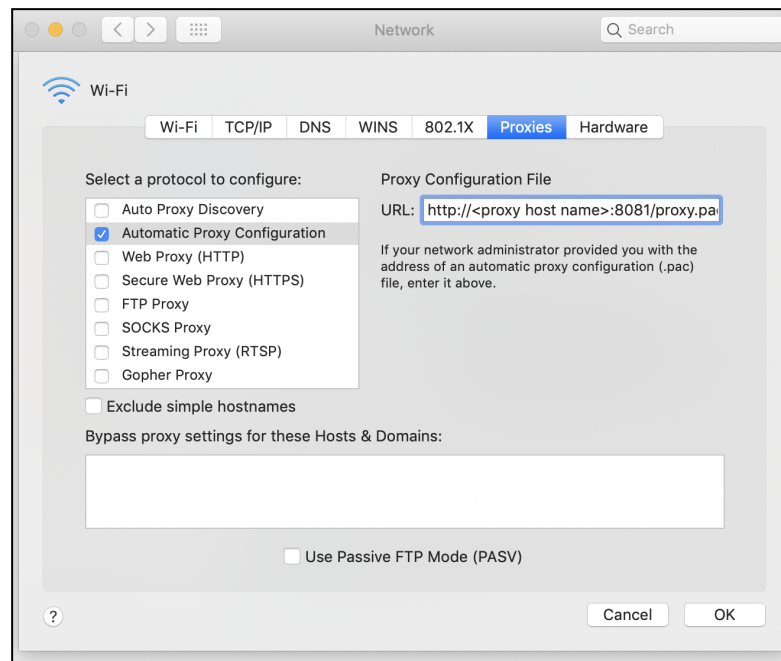
3. Click Save.

In Safari on Mac:

1. Go to Preferences... and display the Advanced tab.
2. In Proxies, click Change Settings.
3. Under Select a protocol to configure, select Automatic Proxy Configuration.
4. Under Proxy Configuration File, make sure the URL field is filled with the following:



http://<proxy host name>:8081/proxy.pac



3.6.1.4 Defining Firewall Rules

Open the following firewall ports for the Symantec Threat Isolation Explicit Proxy topology.

Table 2 Firewall Rules for Symantec Threat Isolation Explicit Proxy

From	To	Protocol	Port	Task
Symantec Threat Isolation Platform (Mandatory)				
Admin Terminal	All Threat Isolation Gateways	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	9000	Administrator access to the Management portal
All Threat Isolation Gateways, including Management	PDP	TCP	3004 3005	Symantec Threat Isolation control protocol for policy distribution



From	To	Protocol	Port	Task
End User Browser	TIE	TCP	80/443	Accessing Threat Isolation Engine (TIE) server from LAN endpoints
End User Browser	Proxy	TCP	8080	Proxying HTTP/S requests. The port is configurable. For assistance, contact Symantec Threat Isolation technical support
End User Browser	Proxy	TCP	8081	Downloading PAC file
End User Browser	Proxy	TCP	HTTP/S 80/443	Downloading resources, for example index.html, Symantec Threat Isolation propriety protocol logic
Report Server	All Threat Isolation Gateways	TCP	6380	Logging and report data
Management	PDP	TCP	9100 9101	Symantec Threat Isolation control protocol for policy distribution
Proxy	External DNS server	UDP	DNS 53	URL resolution
Proxy	Internet	TCP	HTTP/S 80/443	<ul style="list-style-type: none">■ Enables Proxy Internet browsing, i.e. for Bypass/Inspect websites. The ports are mandatory. For websites that listen to higher ports, also open the higher ports (according to your organization's policy)■ If there is no next hop proxy, the proxy must access the Internet via port 80/443 or higher



From	To	Protocol	Port	Task
Proxy	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables Threat Isolation Proxy Internet browsing for non-isolated content when there is a proxy between Threat Isolation Proxy and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings"
TIE	External DNS server	UDP	DNS 53	URL resolution
TIE	Internet	TCP	HTTP/S 80/443	<ul style="list-style-type: none">■ Enables TIE Internet browsing. The ports are mandatory. For websites that listen to higher ports, also open the higher ports (according to your organization's policy)■ If there is no next hop proxy, the TIE must access the Internet via port 80/443 or higher
TIE	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables TIE Internet browsing when there is a proxy between TIE and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings"
Integration with External Servers				
Management	AD	TCP	389	Enables LDAP Queries
Proxy	AD	TCP	LDAP/S 389/636	Enables LDAP authentication



From	To	Protocol	Port	Task
Proxy	AD	UDP	Kerberos 88	Enables Kerberos authentication
Management	IdP	TCP	80/443	Enables IdP Metadata to be imported from a URL. For more information, see section 4.5.4 "Defining SAML Trust"
Proxy/TIE	RADIUS	UDP	Configurable (No default port)	Enables RADIUS authentication. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers"
Proxy/TIE	Email	TCP	Configurable Default = 465	For more information, see section 4.12 "Configuring Email Servers"
Proxy/TIE	SNMP	UDP	162	Port 162 is the default port for sending traps to the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
SNMP	Proxy/TIE	UDP	161	Port 161 is the default listening port for "Expose system metrics" in response to SNMP Walk/GET requests by the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
Management	Syslog	TCP/UDP Default = UDP	Configurable Default = 514	Enables Syslog logging. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers" 4.14 "Configuring Syslog Servers"
Management	ArcSight	TCP/UDP Default = UDP	Configurable Default = 514	Enables ArcSight logging. For more information, see section 4.15 "Configuring ArcSight Servers"



From	To	Protocol	Port	Task
Management	Kafka	TCP	Configurable (No default port)	Enables Kafka logging. For more information, see section 4.16 "Configuring Apache Kafka Servers"

3.6.2 Configuring Symantec Threat Isolation with Downstream Proxy Forwarding

Note

It is recommended to use Symantec Secure Web Gateway (ProxySG) as your downstream proxy. As products from the same vendor, Symantec Threat Isolation and Symantec ProxySG can be integrated smoothly. This convenience is not available when using any other product.

If your organization's endpoints communicate indirectly with the Threat Isolation Proxy through a downstream proxy, the proxy forwarding policy in your downstream proxy must support rule-based definition.

In this topology, endpoint communication with the Threat Isolation Proxy and the TIE is carried by the downstream proxy responsible for the forwarding.

The downstream proxy forwards traffic to one or more selected Threat Isolation Gateway clusters (see section [4.7.12 "Defining Gateway Clusters"](#)) using proxy chaining.

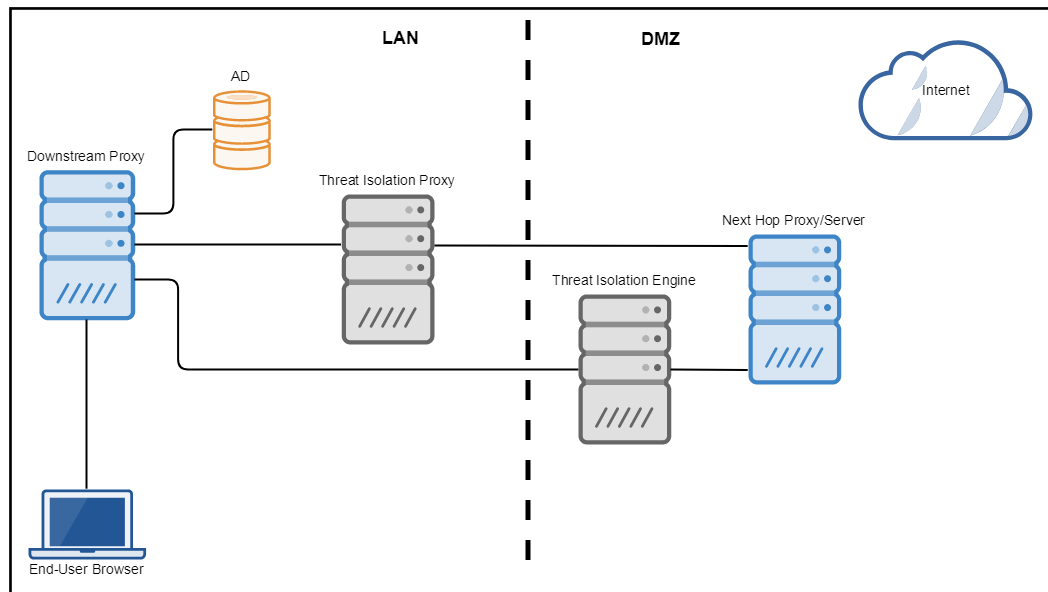


Figure 9 Proxy Chaining

As shown in the figure, the Symantec Threat Isolation Platform distinguishes between two types of third-party proxies, according to their location in relation to the Gateway: the downstream proxy resides between the endpoint and the Threat Isolation Proxy, while the next hop proxy/server resides between the Gateway and the Internet.

For simplicity, the figure [Authentication Mode](#) contains just one next hop proxy/server. Real-life topologies can contain multiple next hop proxies/servers, with the Threat Isolation Proxy and the Threat Isolation Engine (TIE) pointing to different next hop proxy/server machines.

Note that a downstream proxy can act as both downstream proxy and next hop proxy/server on the same machine, as illustrated in the figure [Downstream and Next Hop Proxy/Server on Same Machine](#). In this case, the policy will be run twice: once before the request is forwarded to the Symantec Threat Isolation Platform, and again before it is forwarded to the Internet.

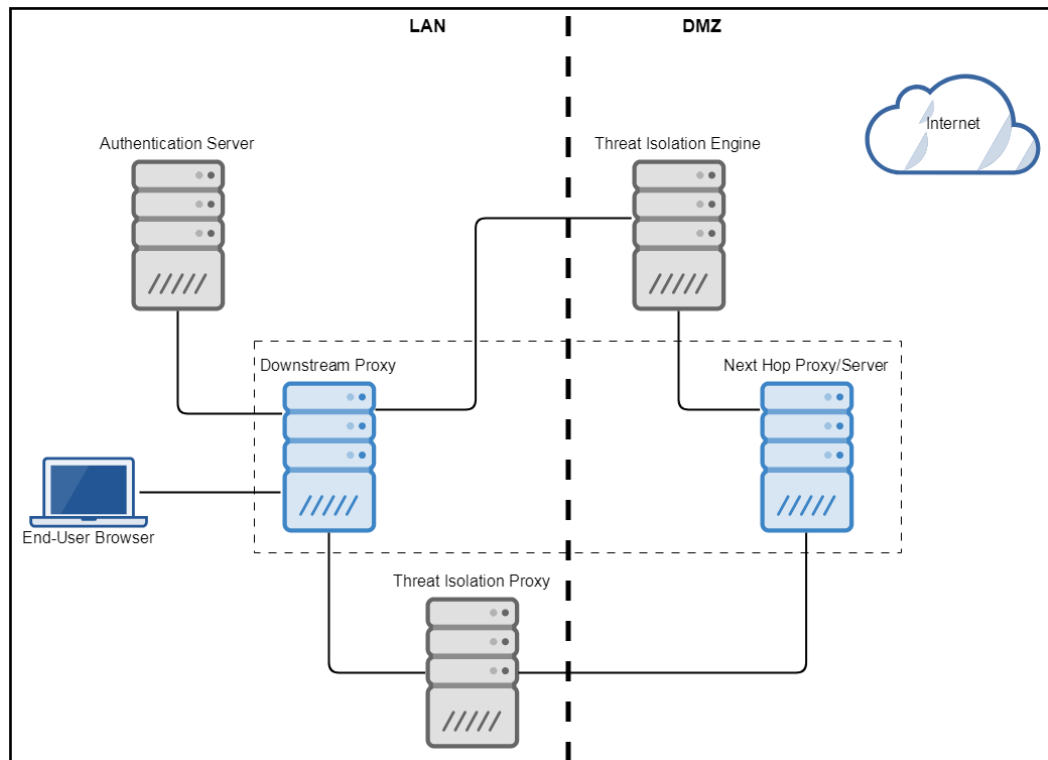


Figure 10 Downstream and Next Hop Proxy/Server on Same Machine

Since the downstream proxy resides between the endpoints and the Threat Isolation Gateway, it must preserve the original data of the source IP and the authenticated user. This data is contained in the following standard request headers:

- X-Forwarded-For (XFF) header – Contains the originating IP address for which the request was forwarded. The downstream proxy adds the XFF header to the request before forwarding it to the Threat Isolation Proxy.
- X-Authenticated-User (XAU) header – Signifies that the downstream proxy has authenticated the end user who originated the request. The downstream proxy adds the XAU header to the request before forwarding it to the Threat Isolation Proxy.
- X-Authenticated-Group (XAG) header – Signifies that the downstream proxy has authenticated the group that originated the request. The downstream proxy adds the XAG header to the request before forwarding it to the Threat Isolation Proxy.



3.6.2.1 Configuring the Downstream Proxy for Communication over HTTPS

If the Symantec Secure Web Gateway (ProxySG) is your downstream proxy, the configuration described in this section can be performed semi-automatically by running scripts that Symantec Threat Isolation generates. This convenience is not available when any other product is used.

Adding forwarding hosts to the downstream proxy

In the downstream proxy, you need to define a number of hosts as forwarding hosts, per Threat Isolation Gateway.

SSL Inspection

If the downstream proxy performs SSL inspection, you need to add the CA certificate defined in section [3.4.4 "Signing the CA Certificate"](#) to your downstream proxy.

Adding rules to the downstream proxy for HTTPS

To support this, add the following rules to the rule base of the downstream proxy when configured for HTTPS.

Table 3 Downstream Proxy Rules for HTTPS

Destination	HTTPS Action	Comment
http://<TIE>/* (URL Regex)	Proxy to TIE:80	Internal Symantec Threat Isolation communication
TIE (hostname)	Proxy to TIE:443	Internal Symantec Threat Isolation communication
Any	Proxy to Threat Isolation Proxy:8080	

3.6.2.2 Configuring the Downstream Proxy for Communication over HTTP

If the Symantec Secure Web Gateway (ProxySG) is your downstream proxy, the configuration described in this section can be performed semi-automatically by running scripts that Symantec Threat Isolation generates. This convenience is not available when any other product is used.

Adding rules to the downstream proxy for HTTP

Add the following rules to the rule base of the downstream proxy when configured for HTTP only.

**Table 4 Downstream Proxy Rules for HTTP**

Destination	HTTP Action	Comments
TIE (hostname)	Proxy to Threat Isolation Engine (TIE):80	Internal Symantec Threat Isolation communication
Any	Proxy to Threat Isolation Proxy:8080	

3.6.2.3 Defining Firewall Rules

Open the following firewall ports for the Symantec Threat Isolation with Downstream Proxy Forwarding topology.

Note:

In this deployment scenario, there is a downstream proxy and a Threat Isolation Proxy. The Threat Isolation Proxy is denoted as the Proxy in the following table.

Table 5 Firewall Rules for Symantec Threat Isolation with Downstream Proxy Forwarding

From	To	Protocol	Port	Task
Admin Terminal	All Threat Isolation Gateways	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	9000	Administrator access to the Management portal
All Threat Isolation Gateways including Management	PDP	TCP	3004 3005	Symantec Threat Isolation control protocol for policy distribution
Downstream proxy	TIE	TCP	80/443	Accessing Threat Isolation Engine (TIE) server from LAN endpoints
Downstream proxy	Proxy	TCP	8080 ^[1]	Proxying HTTP/S requests

[1] This port is customizable. For assistance, contact Symantec Threat Isolation technical support.



From	To	Protocol	Port	Task
Downstream proxy	Proxy	TCP	HTTP/S 80/443	Downloading resources, for example index.html, Symantec Threat Isolation propriety protocol logic
Logging & Report Server	All Threat Isolation Gateways	TCP	6380	Logging and report data
Management	PDP	TCP	9100 9101	Symantec Threat Isolation control protocol for policy distribution
Proxy	External DNS server	UDP	DNS 53	URL resolution
Proxy	Internet	TCP	HTTP/S 80/443	<ul style="list-style-type: none">■ Enables Proxy Internet browsing for Bypass/Inspect websites. The ports are mandatory. For websites that listen to higher ports, also open the higher ports (according to your organization's policy)■ If there is no next hop proxy, the proxy must access the Internet via port 80/443 or higher
Proxy	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables Threat Isolation Proxy Internet browsing for non-isolated content when there is a proxy between Threat Isolation Proxy and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings"
TIE	External DNS server	UDP	DNS 53	URL resolution



From	To	Protocol	Port	Task
TIE	Internet	TCP	HTTP/S 80/443	<ul style="list-style-type: none">■ Enables TIE Internet browsing. These ports are mandatory. For websites that listen to higher ports, also open the higher ports (according to your organization's policy)■ If there is no next hop proxy, the TIE must access the Internet via port 80/443 or higher
TIE	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables TIE Internet browsing when there is a proxy between TIE and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings"

Integration with External Server				
Management	AD	TCP	389	Enables LDAP Queries
Proxy	AD	TCP	LDAP/S 389/636	Enables LDAP authentication
Proxy	AD	UDP	Kerberos 88	Enables Kerberos authentication
Management	IdP	TCP	80/443	Enables IdP Metadata to be imported from a URL. For more information, see section 4.5.4 "Defining SAML Trust"
Proxy/TIE	RADIUS	UDP	Configurable (No default port)	Enables RADIUS authentication. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers"
Proxy/TIE	Email	TCP	Configurable Default = 465	For more information, see section 4.12 "Configuring Email Servers"



Integration with External Server				
Proxy/TIE	SNMP	UDP	162	Port 162 is the default port for sending traps to the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
SNMP	Proxy/TIE	UDP	161	Port 161 is the default listening port for "Expose system metrics" in response to SNMP Walk/GET requests by the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
Management	Syslog	TCP / UDP Default = UDP	Configurable Default = 514	Enables Syslog logging. For more information, see section 4.14 "Configuring Syslog Servers"
Management	ArcSight	TCP / UDP Default = UDP	Configurable Default = 514	Enables ArcSight logging. For more information, see section 4.15 "Configuring ArcSight Servers"
Management	Kafka	TCP	Configurable (No default port)	Enables Kafka logging. For more information, see section 4.16 "Configuring Apache Kafka Servers"

3.6.3 Configuring Symantec Threat Isolation with Block Page Integration

3.6.3.1 Configuring the NGFW/SWG to Redirect Traffic to the Isolation Portal

When a next-generation firewall (NGFW), or a Secure Web Gateway (SWG) without selective forwarding capability that acts as a downstream proxy, resides between the organization's endpoints and the Threat Isolation Proxy, the NGFW/SWG can be configured to redirect traffic to the Isolation Portal. For more information, see section [2.6.4 "Symantec Threat Isolation with Block Page Integration"](#).

Note

This topology is not recommended for use with categories of websites that apply Content Security Policy (CSP), such as social networks like Facebook.com. CSP might not allow resources to be redirected. If traffic cannot be redirected to the Isolation Portal, there will be connectivity issues.



To enable using this topology, configure the following:

1. Go to:

System Configuration → Gateway Advanced Settings → New Gateway Advanced Setting

For more information, see section [4.7.8 "Defining Gateway Advanced Settings"](#).
2. Select the Portal Settings checkbox.
3. Make sure the Show address bar checkbox is clear.
4. In the NGFW or SWG, set the block page redirect URL to redirect to the Isolation Portal. For example:

`https://<isolation-portal-host>?url=<web-site-url>`

3.6.3.2 Placing a Transparent SWG between NGFW and Threat Isolation

When a next-generation firewall (NGFW), or a Secure Web Gateway (SWG) without selective forwarding capability that acts as a downstream proxy, resides between the organization's endpoints and the Threat Isolation Proxy, a transparent SWG (such as Symantec ProxySG) with forwarding capability can be placed between the NGFW and the Proxy. This is also recommended for use with categorized websites, such as social networks.

To use this topology, define the SWG as the downstream proxy. For more information, see section [4.10.1 "Creating New Downstream Proxy Settings"](#).

3.6.3.3 Defining Firewall Rules

Open the following firewall ports for the Symantec Threat Isolation with Block Page Integration topology.

Table 6 Firewall Rules for Symantec Threat Isolation with Block Page Integration

From	To	Protocol	Port	Task
Admin Terminal	All Threat Isolation Gateways	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	9000	Administrator access to the Management portal



From	To	Protocol	Port	Task
All Threat Isolation Gateways including Management	PDP	TCP	3004 3005	Symantec Threat Isolation control protocol for policy distribution
End User Browser	TIE	TCP	80/443	Accessing TIE server from LAN endpoints
End User Browser	TIE	TCP	HTTP/S 80/443	Downloading resources, for example index.html, Symantec Threat Isolation propriety protocol logic
Logging & Report Server	All Threat Isolation Gateways	TCP	6380	Logging and report data
Management	PDP	TCP	9100 9101	Symantec Threat Isolation control protocol for policy distribution
TIE	External DNS server	UDP	DNS 53	URL resolution
TIE	Internet	TCP	HTTP/S 80/443	Enables Threat Isolation Engine (TIE) Internet browsing. These ports are mandatory. For websites that listen to higher ports, you must also open the higher ports (according to your organization's policy).
TIE	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables TIE Internet browsing when there is a proxy between TIE and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings" .

Integration with External Server				
Management	AD	TCP	389	Enables LDAP Queries
Proxy	AD	TCP	LDAP/S 389/636	Enables LDAP authentication



Integration with External Server				
Proxy	AD	UDP	Kerberos 88	Enables Kerberos authentication
Management	IdP	TCP	80/443	Enables IdP Metadata to be imported from a URL. For more information, see section 4.5.4 "Defining SAML Trust"
Proxy/TIE	RADIUS	UDP	Configurable (No default port)	Enables RADIUS authentication. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers"
Proxy/TIE	Email	TCP	Configurable Default = 465	For more information, see section 4.12 "Configuring Email Servers"
Proxy/TIE	SNMP	UDP	162	Port 162 is the default port for sending traps to the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
SNMP	Proxy/TIE	UDP	161	Port 161 is the default listening port for "Expose system metrics" in response to SNMP Walk/GET requests by the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
Management	Syslog	TCP / UDP Default = UDP	Configurable Default = 514	Enables Syslog logging. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers" , 4.14 "Configuring Syslog Servers"
Management	ArcSight	TCP / UDP Default = UDP	Configurable Default = 514	Enables ArcSight logging. For more information, see section 4.15 "Configuring ArcSight Servers"
Management	Kafka	TCP	Configurable (No default port)	Enables Kafka logging. For more information, see section 4.16 "Configuring Apache Kafka Servers"



3.6.4 Configuring Symantec Email Threat Isolation

In the Symantec Email Threat Isolation topology, Symantec Threat Isolation protects email recipients from emails containing links to high-risk and phishing websites. The link is rewritten so that the email recipient is redirected to an Isolation Portal, where the requested website is isolated. For more information, see section [2.5 "Protection Scenarios"](#).

In this topology, the Isolation Portal does not use authentication. Instead, the Email Threat Isolation API signs the URL with a token string that is appended to the URL. Once the isolation instance has verified the token, it gives the client a session cookie used for authorization.

When Symantec Threat Isolation is integrated with the Symantec Messaging Gateway (SMG), you must configure the Threat Isolation Gateway to use token authorization.

To enable using this topology, configure the following:

1. Go to:
`System Configuration > Gateway Advanced Settings`
2. Select the Portal Settings checkbox.
3. Make sure the Show address bar checkbox is clear.
4. In Advanced > Internal Settings, configure the Gateway to use token authorization by selecting the parameter `portal.use_token_authorization`.

For more information, see section [4.7.8 "Defining Gateway Advanced Settings"](#).

3.6.4.1 Defining Firewall Rules

Open the following firewall ports for the Symantec Email Threat Isolation topology:

- If Symantec Threat Isolation is integrated with the Symantec Messaging Gateway (SMG), open all firewall ports described in [Firewall Rules for Symantec Email Threat Isolation](#).
- If Symantec Threat Isolation is integrated with the Symantec Email Security Services (ESS), open only firewall port 443, to enable access to email-isolation.prod.fire.glass.

**Table 7 Firewall Rules for Symantec Email Threat Isolation**

From	To	Protocol	Port	Task
Admin Terminal	All Threat Isolation Gateways	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	9000	Administrator access to the Management portal
All Threat Isolation Gateways including Management	PDP	TCP	3004 3005	Symantec Threat Isolation control protocol for policy distribution
End User Browser	TIE	TCP	80/443	Accessing the Threat Isolation Engine (TIE) server from LAN endpoints
End User Browser	TIE	TCP	HTTP/S 80/443	Downloading resources, for example index.html, Symantec Threat Isolation propriety protocol logic
Logging & Report Server	All Threat Isolation Gateways	TCP	6380	Logging and report data
Management	PDP	TCP	9100 9101	Symantec Threat Isolation control protocol for policy distribution
TIE	External DNS server	UDP	DNS 53	URL resolution
TIE	Internet	TCP	HTTP/S 80/443	<ul style="list-style-type: none">■ Enables Threat Isolation Engine (TIE) Internet browsing■ These ports are mandatory. For websites that listen to higher ports, you must also open the higher ports (according to your organization's policy)



From	To	Protocol	Port	Task
TIE	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables TIE Internet browsing when there is a proxy between TIE and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings"
Integration with External Server				
Management	AD	TCP	389	Enables LDAP Queries
Management	IdP	TCP	80/443	Enables IdP Metadata to be imported from a URL. For more information, see section 4.5.4 "Defining SAML Trust"
Management	RADIUS	UDP	Configurable (No default port)	Enables RADIUS authentication. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers"
TIE	Email	TCP	Configurable Default = 465	For more information, see section 4.12 "Configuring Email Servers"
TIE	SNMP	UDP	162	Port 162 is the default port for sending traps to the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
SNMP	TIE	UDP	161	Port 161 is the default listening port for "Expose system metrics" in response to SNMP Walk/GET requests by the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
Management	Syslog	TCP/UDP Default = UDP	Configurable Default = 514	Enables Syslog logging. For more information, see section 4.14 "Configuring Syslog Servers"
Management	ArcSight	TCP/UDP Default = UDP	Configurable Default = 514	Enables ArcSight logging. For more information, see section 4.15 "Configuring ArcSight Servers"
Management	Kafka	TCP	Configurable (No default port)	Enables Kafka logging. For more information, see section 4.16 "Configuring Apache Kafka Servers"



3.6.5 Configuring Symantec Threat Isolation as Web Application Isolation Gateway Mode

3.6.5.1 Defining Firewall Rules

Open the following firewall ports for the Symantec Threat Isolation as Web Application Isolation Gateway Mode topology.

Table 8 Firewall Rules for Symantec Threat Isolation as Web Application Isolation Gateway Mode

From	To	Protocol	Port	Task
Admin Terminal	All Threat Isolation Gateways	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	SSH 22	Administrator SSH access to the server
Admin Terminal	Management	TCP	9000	Administrator access to the Management portal
All Threat Isolation Gateways including Management	PDP	TCP	3004 3005	Symantec Threat Isolation control protocol for policy distribution
End User Browser	TIE	TCP	80/443	Accessing the Threat Isolation Engine (TIE) server from LAN endpoints
End User Browser	TIE	TCP	HTTP/S 80/443	Downloading resources, for example index.html, Symantec Threat Isolation propriety protocol logic
Logging & Report Server	All Threat Isolation Gateways	TCP	6380	Logging and report data
Management	PDP	TCP	9100 9101	Symantec Threat Isolation control protocol for policy distribution
TIE	External DNS server	UDP	DNS 53	URL resolution



From	To	Protocol	Port	Task
TIE	Internet	TCP	HTTP/S 80/443	<ul style="list-style-type: none">■ Enables TIE Internet browsing■ These ports are mandatory. For websites that listen to higher ports, you must also open the higher ports (according to your organization's policy)
TIE	Explicit next hop proxy/server	TCP	HTTP/S 8080	Enables TIE Internet browsing when there is a proxy between TIE and Internet (optional). The port is configurable in the Next Hop Proxy object. For more information, see section 4.11 "Creating New Next Hop Proxy/Server Settings" .
Integration with External Server				
Management	AD	TCP	389	Enables LDAP Queries
Management	IdP	TCP	80/443	Enables IdP Metadata to be imported from a URL. For more information, see sections 4.6.2.1 "Creating RADIUS Identity Providers" , 4.5.4 "Defining SAML Trust"
Management	RADIUS	UDP	Configurable (No default port)	Enables RADIUS authentication. For more information, see section 4.6.2.1 "Creating RADIUS Identity Providers"
TIE	Email	TCP	Configurable Default = 465	For more information, see section 4.12 "Configuring Email Servers"
TIE	SNMP	UDP	162	Port 162 is the default port for sending traps to the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"
SNMP	TIE	UDP	161	Port 161 is the default listening port for "Expose system metrics" in response to SNMP Walk/GET requests by the SNMP server. For more information, see section 4.13 "Configuring SNMP Servers"



From	To	Protocol	Port	Task
Management	Syslog	TCP/UDP Default = UDP	Configurable Default = 514	Enables Syslog logging. For more information, see section 4.14 "Configuring Syslog Servers"
Management	ArcSight	TCP/UDP Default = UDP	Configurable Default = 514	Enables ArcSight logging. For more information, see section 4.15 "Configuring ArcSight Servers"
Management	Kafka	TCP	Configurable (No default port)	Enables Kafka logging. For more information, see section 4.16 "Configuring Apache Kafka Servers"

3.6.6 Pushing Settings to the Gateways

After you have completed the initialization process and made all the necessary changes, remember to push the new settings to all Threat Isolation Gateways, as described in section [4.7.6 "Pushing Settings"](#). Now, you can safely browse the web using the Symantec Threat Isolation Platform.

3.7 Viewing Version and License Information, Credits

The About Symantec Threat Isolation dialog contains version and license key information, as well as links to the License Agreement and the Acknowledgments window. The Acknowledgments window lists the authors of open-source packages used by Symantec Threat Isolation.

To display the About Symantec Threat Isolation dialog, click the vertical ellipsis in the menu bar and then choose About...

3.8 Moving Management to a Different Server

If you need to move the Symantec Threat Isolation Management to a different server, you will need to reinstall it on the new machine. For more information, see section [3.5.7 "Defining the Management Gateway"](#).

3.9 Upgrading the Symantec Threat Isolation System

When you receive notification that a Symantec Threat Isolation upgrade is available, perform the relevant procedure below to upgrade your Symantec Threat Isolation Proxies and application. Note that during the upgrade process, the Threat Isolation Gateway will be down briefly while it updates itself to be able to run the new version.



3.9.1 Upgrading from Version 1.10 to Version 1.13

Perform the following to upgrade your Symantec Threat Isolation Proxies and application from version 1.10 to version 1.13:

- If you want to use the Cloud, type:

```
sudo fgcli system upgrade <X.X.X+Y>
```

where X.X.X+Y is the full version name of the required build.
For example, 1.13.7+1143.

- If you are upgrading from an ISO file, type:

```
sudo fgcli system upgrade <path><file name>.iso
```

- If you are upgrading from a mounted media (DVD), type:

```
sudo mkdir -p /mnt/cdrom  
sudo mount -o loop /dev/cdrom /mnt/cdrom  
sudo fgcli system upgrade /mnt/cdrom
```

3.9.2 Upgrading from Version 1.11 to Version 1.13

Perform the following to upgrade your Symantec Threat Isolation Proxies and application from version 1.11 to version 1.13:

- If you want to use the Cloud, type:

```
sudo fgcli system upgrade to-version <X.X.X+Y>
```

where X.X.X+Y is the full version name of the required build. For example, 1.13.7+1199.

- If you are upgrading from an ISO file, type:

```
sudo fgcli system upgrade from-path <path><file name>.iso
```

- If you are upgrading from a mounted media (DVD), type:

```
sudo mkdir -p /mnt/cdrom  
sudo mount -o loop /dev/cdrom /mnt/cdrom  
sudo fgcli system upgrade from-path /mnt/cdrom
```

3.10 Performing Shutdown

To properly shutdown the Symantec Threat Isolation computer, perform the relevant procedure:

- On a physical appliance, access a command line and enter:

```
sudo shutdown -h now
```

- On a virtual machine (VM), right-click and select Shutdown Guest.



3.11 Performing Backup, Restore and Reset Procedures

3.11.1 Backing Up System Data

1. Log in to the Management machine through SSH.
2. Run the following command:

```
fgcli management backup -o <back-up location path>
```

Note

The location path must be under `/var/cache/fireglass/management`.

3. Enter Y to confirm the backup.

A system-generated filename is displayed. Record the filename for future usage.

Notes

- Backing up data using the `fgcli` command only saves the data locally on the Management machine. To store the data in another location, copy the file to the new location.
- You can also backup your data to the AWS cloud. This requires your own AWS account, additional firewall settings and access. To setup an automatic backup system or an AWS cloud backup system, contact Symantec Threat Isolation technical support.
- Only the Management database is backed up via the backup procedure; activity logs, event logs and audit logs are not. To backup such logs, forward them to an external log server (Syslog, Kafka or ArcSight). The data will be saved there, but cannot be imported back into the Symantec Threat Isolation Management console.

3.11.2 Restoring System Data

1. Access the Management machine and type the command:

```
fgcli management restore -m full -i <filename to restore>
```
2. Enter Y to confirm the restore.

A confirmation message is displayed when the system is restored.
3. Push settings.



3.11.3 Resetting a Management User Password

You can reset a Management user password from outside of the Management console by running fgcli, as follows:

1. Type the command:

```
fgcli management reset-admin-password
```

2. Specify the new password:

```
<supply a new password>
```

See section [3.11.3.1 "Password Policy"](#) for a detailed explanation of the password policy.

3. Retype the new password:

```
<supply the same password again>
```

3.11.3.1 Password Policy

Symantec Threat Isolation validates passwords according to two criteria:

- Minimal length: 0 - 255 characters (default: 8)

Any character is valid.

- Minimal strength: 0 - 4 (default: 3)

Strength levels are:

0 - Poor

1 - Weak

2 - Medium

3 - Strong

4 - Very Strong

Symantec Threat Isolation uses internal logic to evaluate the strength level of a password. For example, the evaluating component recognizes dictionary words, patterns and repetitions, and therefore might not accept a password that you consider strong. In such cases, the reason for the rejection will be given.

The password policy is enforced only in new passwords; passwords of existing users can remain as they were. When the password of an existing user is changed, the new password must comply with the policy.



If your organization does not want Symantec Threat Isolation to enforce password strength, you can change the default configuration as follows:

1. Go to:
`System Configuration > Advanced Configuration`
2. Edit the following parameters:
 - ◆ `authenticationService.passwordPolicy.minimumLength` - minimum password length
 - ◆ `authenticationService.passwordPolicy.minimumStrengthScore` - minimum password strength level

Note

Changing the password policy configuration affects the password policy of both Management users and internal users (see section [4.6.1 "Creating Management Users"](#) and section [4.5.1.1 "Creating Internal Users"](#)).

3.11.4 Restoring the Default Settings

To return to the default settings of a new installation (system reset):

1. Log in to the Management machine through SSH.
2. Run the following command:
`fgcli management restore -m factory_default`
3. Enter Y to confirm the system reset.

This restores the initial machine settings. Now, run the First Time Wizard and the corresponding settings to complete the installation (see section ["3.5.7 "Defining the Management Gateway"](#)).

Note

All credentials are reset during the system reset procedure. In the First Time Wizard, use the username and password admin/admin.

For more information, see the following sections:

- ["3.5.6 "Initializing the Symantec Threat Isolation Platform"](#)
- ["3.5.11 "Installing the CA Certificate as Trusted Root CA on the Client Side"](#)
- ["3.5.12 "Verifying the Trusted Root CA in the Endpoint Browser"](#)



4 Configuring Security Policy Settings

4.1 Overview

The following diagram illustrates the hierarchy of the Symantec Threat Isolation system security policy distribution.

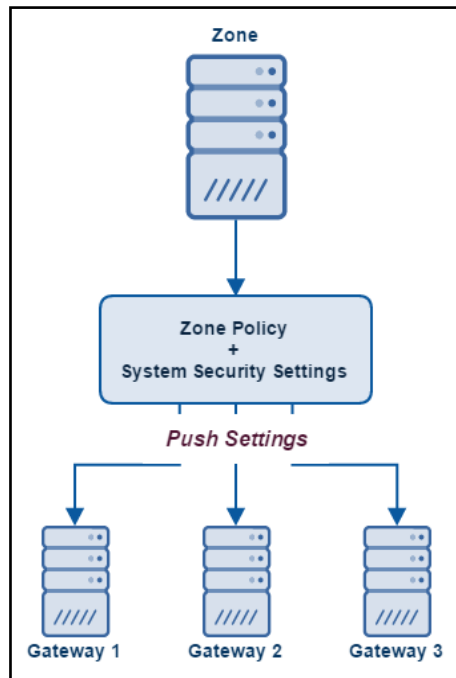


Figure 11 System Security Policy Distribution Hierarchy

In the Symantec Threat Isolation system, a Zone represents a server farm made up of multiple Threat Isolation Gateways. Currently, Symantec Threat Isolation supports a single Zone, the default Primary Zone, which is available out of the box. For more information, see section [4.7.2 "Configuring the Zone"](#).

A number of Gateways are associated with a Zone. Each defined Gateway can function in various ways, for example as a Threat Isolation Proxy, Threat Isolation Engine (TIE), or Management server, and can be connected to multiple internal and external servers, such as Internet, DNS, AD, mail, or other servers.

Each Zone has a single security policy defined for it. This security policy consists of a policy rule base – a number of policy rules that are enforced on a first-match basis. For a description of security policies, see section [4.2 "Defining Security Policies and Rules"](#).

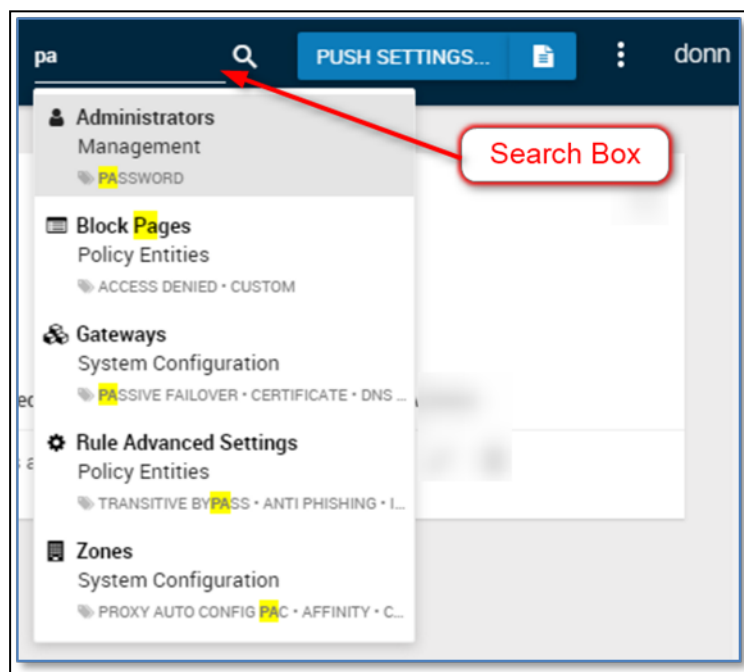


The security policy defined for a particular Zone is applied to all Gateways that are associated with that Zone using the Push Settings function. Each time the policy is updated or new rules are defined, the changes must be pushed again. For a description of Gateways, their functions, and policy distribution, see section [4.7 "Defining Zones, Gateways, and Associated Components"](#).

4.2 Defining Security Policies and Rules

4.2.1 Menu Search

To locate items quickly within Symantec Threat Isolation, type the selection in the Menu Search box on the top right of all screens. The search box only requires partial matching to begin listing the search results.



4.2.2 Editing Your Policy

This section explains how to edit the policy that Symantec Threat Isolation creates automatically when you define the Management Gateway, using the First Time Wizard.

1. To access Symantec Threat Isolation security policies, go to:
Policies → All Policies



2. Do one of the following:

- ◆ To edit a policy on the All Policies page:

Under Actions, click the edit icon for the specific policy.

- ◆ To edit a specific policy page, such as My Policy:

Click the edit icon beside the policy name at the top left of the page.

3. Edit the parameters described in the table below, and then click Update.

Parameter	Description	For More Information
General		
SSL Interception	Select to intercept SSL traffic	
Authentication Settings		
Use Authentication	Select to enable authentication	
Mode	Select the method of authentication: via proxy or via server	For information about authentication mode considerations, see section 4.2.2.2 "Authentication Mode"
Profile	Select the authentication profile: Active Directory, Internal identity or SAML	<ul style="list-style-type: none">■ For a description of the available authentication profiles, see section 4.2.2.1 "Defining Authentication Profiles"■ For Active Directory settings, see section 4.5.2 "Defining Active Directory Settings"■ For information about defining internal users, see section 4.5.1.1 "Creating Internal Users"■ For SAML settings, see section 4.5.4 "Defining SAML Trust"



Parameter	Description	For More Information
Obtain user identity via X-Authenticated-User header	This mode is relevant when a downstream proxy rather than the Threat Isolation Proxy performs the authentication and sends the user identity to the Threat Isolation Gateway in the standard XAU header. This option appears selected or clear automatically, according to the settings defined for the X-Authenticated-User (XAU) Header in the Downstream Proxy Settings object	See section 4.10.1 "Creating New Downstream Proxy Settings"
Authentication Caching		
Apply Authentication caching for non-browser applications by source IP	Select to enable authentication caching	See section 4.2.2.3 "Authentication Caching"
System Rules		



Parameter	Description	For More Information
Authenticate system rules	<p>Select to make the Gateway try to authenticate the user who made a request that was matched with a system rule.</p> <p>To enable system rules authentication, the value of the User field in the default rules for the relevant browsers/non-browser applications must be changed from “Any” to “All Authenticated users”.</p> <p>NOTE: Some system rules cannot be authenticated. Therefore, the above will not affect them.</p> <p>When the Authenticate system rules box is clear (default), the Gateway will not try to authenticate the user who made a request that was matched with a system rule, even if in the relevant default rules, the value of the User field is “All Authenticated users”. Default: False</p>	<p>See section 4.2.2.4 "System Rules"</p> <p>See section 4.2.7 "Defining Policy Rules"</p>
Enable system rules Activity logs	Select to generate an activity log whenever a system rule is matched. Default: False	See section 4.2.2.4 "System Rules"
Allow access to common authentication services from non-browser applications, such as Google OAuth 2.0	Select to allow access to common authentication services from non-browser applications, such as Google OAuth 2.0. Default: True	
Advanced		



Parameter	Description	For More Information
Advanced Settings	Enables editing of policy's advanced internal settings. NOTE: Contact Symantec Threat Isolation technical support for assistance with these settings	See section 4.4.11 "Creating Policy Advanced Settings"

4.2.2.1 Defining Authentication Profiles

The Symantec Threat Isolation Platform provides four authentication profiles out of the box. Currently, these profiles are fixed; they cannot be updated. The following table describes the available authentication profiles.

Parameter	Description	Authentication Mode	For More Information
Active Directory	Enforces authentication based on users listed in the Active Directory database	Proxy or Server	See section 4.5.2 "Defining Active Directory Settings"
Internal Identity	Enforces authentication based on end users listed in the Symantec Threat Isolation user directory	Proxy or Server	See section 4.5.1.1 "Creating Internal Users"
SAML Authentication	Enforces SAML authentication	Server	See section 4.5.4 "Defining SAML Trust"
No Authentication	No authentication is enforced. To disable authentication, clear the Use Authentication checkbox		See section 4.2.2 "Editing Your Policy"

4.2.2.2 Authentication Mode

The authentication mode you select depends primarily on your topology. Use the use cases listed in the table below as a guide to assist you with selecting the appropriate authentication mode.

Note

Internal identity authentication and Active Directory authentication can be used in Proxy mode as well as in Server mode; however, SAML must be used in Server mode.



Use Case	Mode	For more information
Symantec Threat Isolation explicit proxy	Proxy	See section 3.6.1 "Configuring the Symantec Threat Isolation Explicit Proxy Topology"
A downstream proxy between the endpoint browser and the Threat Isolation Gateway authenticates the endpoints using the HTTP response: 407 Proxy Authentication Required. In this case, the Gateway must be configured with Server authentication mode. Otherwise, the Gateway can be configured with Proxy authentication mode.	Server	See section 3.6.2 "Configuring Symantec Threat Isolation with Downstream Proxy Forwarding"
Your company uses Web Application Isolation Gateways. NOTE: Web Application Isolation Gateways use Server authentication regardless of the mode with which they are configured.	Server	See section 3.6.3 "Configuring Symantec Threat Isolation with Block Page Integration"
SAML Authentication	Server	See section 4.5.4 "Defining SAML Trust"

Proxy Authentication Mode

In Proxy authentication mode, the Gateway issues a Proxy challenge (HTTP 407) for every new connection.

Note

When a downstream proxy between the browser and the Gateway authenticates the endpoints using the HTTP response: 407 Proxy Authentication Required, the Server authentication mode must be used. For more information, see the section ["Server Authentication Mode"](#) below.

The following flow chart illustrates the initial browsing flow in Proxy authentication mode. Each leg is explained below.





1. The client (browser) surfs to a website on the Internet.
2. Since the Threat Isolation Proxy does not know the user's identity, it returns a standard HTTP response: 407 Proxy Authentication Required (for an explanation, see <https://www.iana.org/assignments/http-status-codes/http-status-codes.xhtml>).

Note

Authentication is required only when the matched rule demands it. For more information, see section [4.2.6 "Match Criteria Flow"](#).

3. The browser gets the identity information from the user or from the OS, then sends the authentication information to the Threat Isolation Proxy.
4. The Threat Isolation Proxy verifies with the identity provider that the user is authenticated. It then returns the 200 OK status that concludes authentication, together with the HTML content. The HTML content depends on the matched rule. For more information, see section [2.2 "Returned HTML Content"](#).

Skipping Authentication when Egress IP Has Been Authenticated

Some applications do not support Proxy authentication. To avoid connectivity issues in such cases, Symantec Threat Isolation allows authentication to be skipped when the source egress IP address (the source IP address that the traffic comes from) has already been authenticated within the configured authentication caching timeout. The policy can be edited to include criteria for skipping authentication.

When these criteria are matched and the source egress IP address was authenticated previously, the user is considered trusted and authentication will be skipped. The activity log displays "Generic User" instead of the user name when user authentication was skipped for unauthenticated requests. In that case, rules with a specific Access Role were skipped during matching.

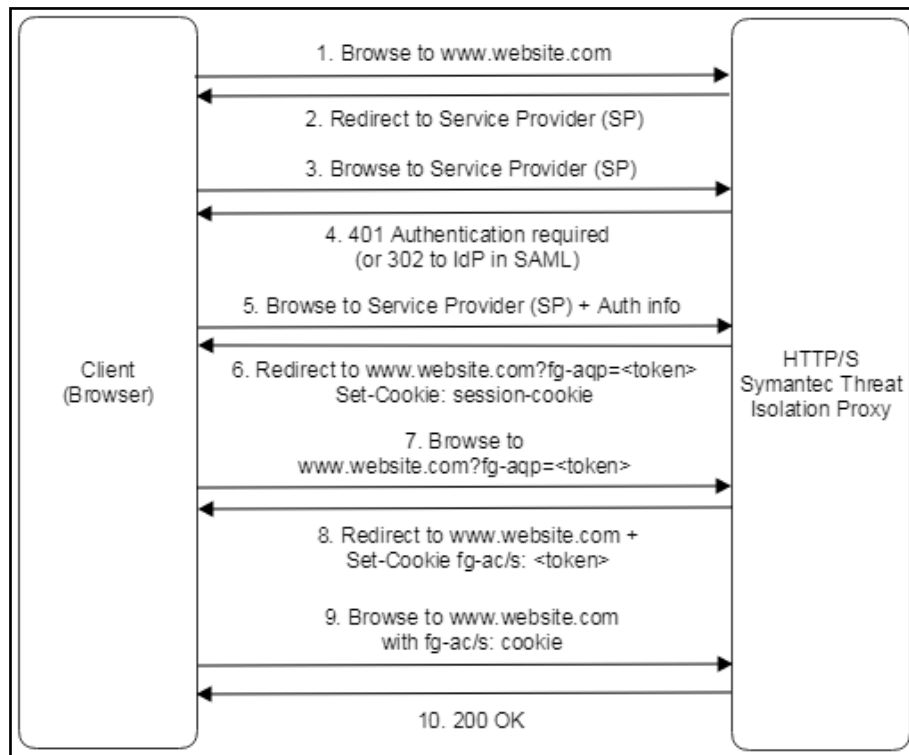
For more information, follow this Symantec support link, and refer to the Proxy Authentication Mode section:

<http://entced.symantec.com/entt?product=wi&version=%2A&language=english&module=authsettings&error=0&build=symantec>

Server Authentication Mode

In Server authentication mode, the Threat Isolation Gateway issues an Authentication challenge (HTTP 401) for every new connection.

The following flow chart illustrates the initial browsing flow in Server authentication mode. Each leg is explained below.



1. The client (browser) surfs to a website on the Internet.
2. The Threat Isolation Proxy configured with the Server authentication mode returns a 302 Redirect to Service Provider (SP) rather than the standard 407 response. (The Service Provider (SP) is the Threat Isolation Proxy.)
3. The browser browses to the Service Provider (SP).
4. Since the Service Provider (SP) does not know the user's identity, it returns 401 Authentication required.

Note

Authentication is required only when the matched rule demands it. For more information, see section [4.2.6 "Match Criteria Flow"](#).

5. The browser gets the identity information from the user or from the OS, then sends the authentication information to Threat Isolation Proxy.
6. The Service Provider (SP) returns a 302 Redirect to the original URL, with a Symantec Threat Isolation query-param that contains a token. It also sets a cookie for persistency. This cookie makes steps 4 and 5 redundant in future requests.
7. The browser asks for the URL provided in step 6, and attaches the token.



8. The Threat Isolation Proxy redirects the browser to the original URL of the requested website. It also sets a cookie for persistency. This cookie makes steps 1-8 redundant in future requests.
9. The browser asks for the original URL of the requested website with a cookie.
10. The Threat Isolation Proxy verifies with the identity provider that the user is authenticated. It then returns the 200 OK status that concludes authentication, together with the HTML content. The HTML content depends on the matched rule. For more information, see section [2.2 "Returned HTML Content"](#).

Skipping Authentication when Egress IP Has Been Authenticated

When a proxy resides in the cloud, it cannot communicate directly with an authentication server that resides in the LAN. If redirect cannot be done in this case, authentication is likely to fail, resulting in connectivity issues for Bypass and Inspect actions. (This is not relevant for isolated web traffic.) Connectivity issues can also be experienced by websites that apply Content-Security-Policy[1] such as Facebook.com.

To address the connectivity issues, Symantec Threat Isolation allows authentication to be skipped when the source egress IP address (the source IP address that the traffic comes from) has already been authenticated within the configured authentication caching timeout. The policy can be edited to include criteria for skipping authentication. When these criteria are matched and the source egress IP address was authenticated previously, the user is considered trusted and authentication will be skipped. The activity log displays "Generic User" instead of the user name when user authentication was skipped for unauthenticated requests. In that case, rules with a specific Access Role were skipped during matching.

For more information, follow this Symantec support link, and refer to the Server Authentication Mode section:

<http://entcd.symantec.com/entt?product=wi&version=%2A&language=english&module=authsettings&error=0&build=symantec>

4.2.2.3 Authentication Caching

A user using a browser or an application that supports proxy authentication is able to authenticate, but a non-browser application that does not support proxy authentication has no means to offer credentials and authenticate.

[1] For more information, see the Wikipedia description of Content-Security-Policy, at: https://en.wikipedia.org/wiki/Content_Security_Policy.



When Authentication Caching is selected, and the user has accessed the Internet with approved credentials, Symantec Threat Isolation caches the username related to the IP address and authenticates all applications from this IP, based on the user.

The following table describes the two types of cached settings:

Parameter	Description	For More Information
Using the last identity learned from the source IP	Caches the last username authentication from the IP address. The user is identified in the activity logs. When Symantec Threat Isolation uses this mode, the username and IP are cached for three hours.	
Without Identity (for example, when users are behind a NAT device)	Using any username authenticated from the source IP, the non-browser application authenticates anonymously (for example, behind a NAT device). The user cannot be identified in the activity logs. When Symantec Threat Isolation uses this mode, authentication is cached for seven days.	

4.2.2.4 System Rules

Browsers and non-browser applications must be able to consume certain Cloud services, such as Microsoft and Google services, to function properly. For your convenience, Symantec has defined implicit system rules to ensure access to the following common Cloud services:

- Google Chrome Omnibox, connectivity probe and search autocomplete
- Updates for browsers and common applications
- Resources required by Microsoft CryptoAPI
- CRL and OCSP access to well-known certificate authorities (configurable)
- Access to common authentication services from non-browser applications, such as Google OAuth 2.0 (configurable)

Note that the Threat Isolation Gateway will try to match these system rules first, before attempting to match rules that are defined explicitly in the policy.

4.2.3 Source Application Policy Rules

Symantec Threat Isolation recognizes the difference between applications that are initiated from a browser, and applications that are not initiated from a browser (for example, an update program from an application). When setting up a rule, you



need to determine which type of application is processed by that rule. Select either Browser, Application or Any, for any type of application from the endpoint. For more information and setup, see section [4.2.7 "Defining Policy Rules"](#). The out-of-the-box setup includes two default closure rules:

- The rule named Default Rule - A browser-initiated application rule. The action is Isolate
- The rule named Default Rule for Applications - A non-browser initiated application rule. The action is Pass

4.2.4 Working with Policies

Working with policies is based on the following definitions:

- Profile – A number of related settings that determine the actions related to the specific security setting:
 - ◆ Isolation: Isolate, Inspect, Block, Pass
 - ◆ Download: Allow, Scan, View or Block download of various file types
 - ◆ Upload: Allow or Block upload of various file types
 - ◆ Activity logging: Defines the type, amount, and depth of data logged for subsequent analysis
 - ◆ User actions: Copy, Paste, Print, Save as
- Rule – An element that contains:
 - ◆ Match criteria (pictured below in the red box) – i.e., User, Source, Destination – that must be matched by the HTTP/S request
 - ◆ Actions criteria (pictured below in the blue box) – for example, browsing, logging, end-user data protection, application data protection, and so on – a combination of different profiles that are enforced when the match criteria are met
 - ◆ Policy – The first match rule base



Order	Name	Active	Client Ap...	User	Source	Destinati...	Action	Downloa...	Logging	Descripti...	Updated ...	Actions
1	Document Isolation ...	<input type="checkbox"/>	Any	Any	Any	* Docu...	Isolate (Grid Ren...	Docu...	Prima...	Documen...	4 days ag...	
2	Default Rule	<input checked="" type="checkbox"/>	Browser: Any	Any	Any	Any	Isolate (Grid Ren...	Prima...	Prima...	Default R...	4 days ag...	
3	Default Rule for App...	<input checked="" type="checkbox"/>	Applicati	Any	Any	Any	Inspect	Prima...	Prima...	Default R...	4 days ag...	

4.2.5 Enforcing Policies

- The security policy is a first-match policy. The Symantec Threat Isolation Platform enforces the policy as follows:
 - ◆ The Symantec Threat Isolation Platform checks the policy's rules one by one to find the first one that matches the request. Once there is a match, the Symantec Threat Isolation Platform enforces that rule.
 - ◆ There is always a closure rule. The closure rule has a default match criterion to include any match. The default verdict is Isolate, but this can be changed by the Management user.
- You can maintain a single security policy for your entire organization, as defined in the out-of-the-box Symantec Threat Isolation default policy, called "My Policy."
- You can define additional policies to meet the security requirements of your organization. If there are multiple policies, the Symantec Threat Isolation Platform Zone checks its Policy field to enforce the correct policy.

Note

It is important to remember that some policies do not require authentication of end users, but might contain rules that do.

4.2.6 Match Criteria Flow

The match criteria of a security rule are evaluated in the following order: Source (first), Destination (second), Request Headers (third), User (fourth).

- If there is a match on all four criteria, Symantec Threat Isolation determines the verdict enacted for the request.
- If there is no match for Source (first), Symantec Threat Isolation does not even check the other three match criteria (Destination, Request Headers, and User). Instead, Symantec Threat Isolation continues to the next rule in the security policy's list.



- If there is a match for Source, Symantec Threat Isolation checks Destination. If there is no match for Destination, Symantec Threat Isolation continues to the next rule. And so it continues for the remaining criteria.
- Authentication is an expensive action that can slow down the browsing experience. Therefore, users are authenticated only if the User criteria specifically require authentication. For more information, see section [4.2.7 "Defining Policy Rules"](#), the User field, and section [9.3.4 "Unauthenticated Users in Activity Logs"](#).

Note

Authentication starts only when all other match criteria are met.

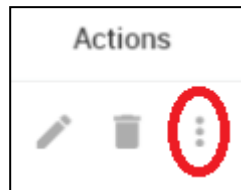
4.2.7 Defining Policy Rules

A security policy is first-match rule based, and contains rules that you define. This section describes how to define the rules that comprise the granular first-match rule base of a policy. For information about match criteria and the order in which they are evaluated, see section [4.2.6 "Match Criteria Flow"](#). For information about rule actions, see section [4.2.7.2 "Rule Actions"](#).

1. To create a policy rule, go to:
`Policies → [your policy]`
2. Do one of the following:
 - ◆ Click New Rule to create a rule. The new rule will be placed at the bottom of the rules in the Policy page.



- ◆ In an existing rule, click the vertical ellipsis Actions item:



From the content menu, select one of the following options:

- Create New Before... to create a rule above the existing rule.
- Create New After... to create a rule below the existing rule.
- Copy to clone the existing rule. Selecting this option displays three additional menu options: Cancel Copy; Create From Copy Before, and Create From Copy After.

Note

To move an existing rule to the top of the [your policy] page, click the vertical ellipsis icon in its row and then select Move To Top from the context menu.

3. Configure the parameters described in the table below for the new security policy rule, and then click Create.

Parameter	Description	For More Information
Match Criteria		
Client Application	<ul style="list-style-type: none">■ Any - The policy rule effects all client traffic■ Browsers - The policy rule effects only traffic generated from the browser■ Applications - The policy rule effects only traffic generated from a non-browser application	



Parameter	Description	For More Information
User	<p>The user supports Access Roles.</p> <p>When creating a new rule, you can select one of the following:</p> <ul style="list-style-type: none">■ Any (including unauthenticated users) - The default option. If the User field is left empty, the rule can be matched without the need to authenticate the user■ All authenticated users - The out-of-the-box Access Role. Authentication is needed; the rule will be matched for any authenticated user■ One or more existing Access Roles. Authentication is needed; the rule will be matched only if the user or group is matched	<p>See section 4.4.3 "Creating Access Roles" for defining Access Roles</p>
Source	<p>The source of the end users, based on network objects or network object groups</p>	<ul style="list-style-type: none">■ See section 4.4.7.1 "Defining Network Objects" for network objects■ See section 4.4.7.2 "Defining Network Object Groups" for network object groups



Parameter	Description	For More Information
Destination	<p>Internal or external destinations (URL Objects, URL Object Groups, URL Categories, Risk Levels, Applications, Network Objects, Network Object Groups and Geolocation Objects)</p> <p>NOTE: When the destination includes at least one application or group of applications, the Isolate action becomes unavailable and the Client Application value is set to Any</p>	<ul style="list-style-type: none">■ See section 4.4.4.1 "Defining URL Categories" for URL categories■ See section 4.4.4.2 "Defining Risk Levels" for Risk Levels■ See section 4.4.5 "Controlling Non-Browser Application Objects" for applications■ See section 4.4.7.1 "Defining Network Objects" for network objects■ See section 4.4.7.2 "Defining Network Object Groups" for network object groups■ See section 4.4.8 "Creating URL Objects and Object Groups" for URL objects■ See section 4.4.8.2 "Creating URL Object Groups" for URL object groups■ See section 4.4.12 "Creating Geolocation Objects" for Geolocation objects
Source Geolocation	<p>Apply this policy rule to specific countries, an internal network or an unknown geolocation.</p> <p>This field is hidden by default, but appears when you click More</p>	<p>See section 4.2.7.1 "Source Geolocations" for source geolocation details</p>



Parameter	Description	For More Information
Request Filters	<p>Specifies the criteria in the HTTP request header to filter by match criteria.</p> <p>This field is hidden by default but appears when you click More</p>	See section 4.4.9 "Creating Request Filters" for defining request filters
Action		
Action	<p>The action you choose will set the policy rule for the selected profile.</p> <p>NOTE: When the destination includes as least one application or group of applications, the Isolate action becomes unavailable and the Client Application value is set to Any</p>	See section 4.3.3.1 "Overview" for isolation profile actions
Activity Log Profile	Defines what end-user actions (such as keystrokes, copied data, printed webpages) and network requests are or are not logged	See section 4.3.6 "Defining Activity Log Profiles"
Isolation Profile	Associates an isolation profile that defines the Isolation settings experience	See section 4.3.3 "Defining Isolation Profiles" for defining isolation profiles
Download Profile	Associates a download profile that defines how downloaded files are handled	See section 4.3.4 "Defining Download Profiles"
Upload Profile	Associates an upload profile that defines how uploaded file types are handled	See section 4.3.5 "Defining Upload Profiles"
The following parameters are additional profile actions:		
Block Page	<ul style="list-style-type: none">■ Relevant when the Isolation Profile = Blocked■ Defines the block page message returned to the end user for blocked content	See section 4.4.6 "Creating Custom Pages"
End-User Data Protection Profile	Associates an End-User Data Protection profile that protects end-user data from potentially malicious websites	See section 4.3.6.3 "URL Query Parameter Privacy"
Application Data Protection Profile	Associates an Application Data Protection profile to protect an organization's application data by controlling how information can leave the application, for example via copying or printing	See section 4.3.8 "Defining Application Data Protection Profiles"



Parameter	Description	For More Information
Anti-Bot Protection	Associates an Anti-Bot Protection profile that prevents bots inside the organization's network from reaching the Internet using the HTTP protocol	See section 4.3.8.3 "Opening Developer Tools Remotely"
Advanced		
Advanced Settings	This selection opens the Rule Advanced Settings window or you can add a new advanced setting rule	See section 4.4.10 "Creating Rule Advanced Settings"
Components	Specifies the relevant components that apply to this rule. Options include: Proxy and Threat Isolation Engine	

4.2.7.1 Source Geolocations

Select one or multiple countries to include for this policy rule. By using Source Geolocation, you can regionalize your policy rules to specific locations by country. The option Internal Network refers to private IP addresses:

- 192.168.1.1 – 192.168.255.254
- 10.0.0.1 – 10.255.255.254
- 172.16.0.1 – 172.31.255.254

Unknown Geolocation refers to those rare IP addresses that are not associated with any geographic region and are therefore unknown.

4.2.7.2 Rule Actions

Four types of actions can be performed on HTTP/S responses. Only isolated or blocked content goes through the Threat Isolation Engine (TIE); all other content goes through the Threat Isolation Proxy. For the Isolate action, you can define Isolation profiles as required by your organization.



The table below defines the Symantec Threat Isolation rule actions.

Action	Description	For More Information
Isolate	<ul style="list-style-type: none">■ The security level is high; HTTP/S responses of this type are always isolated■ The Symantec Threat Isolation Platform checks the WebSocket request and determines that it should be isolated■ The Symantec Threat Isolation Platform translates website content into visible elements and collects user gestures to the isolated virtual browser in the TIE■ The Symantec Threat Isolation Platform isolates the HTTP/S response and sends it to the endpoint browser for display■ The Isolate action requires designation of both a Download Profile and an Upload Profile	<ul style="list-style-type: none">■ See section 4.3.4 "Defining Download Profiles"■ See section 4.3.5 "Defining Upload Profiles"
Inspect	<ul style="list-style-type: none">■ The security level is medium. WebSocket requests of this type are considered neutral■ The action is Inspect only if the downloaded content includes links to downloaded files■ The Inspect action requires definition of a Download Profile■ The Symantec Threat Isolation Platform downloads the HTTP/S response to the server, inspects it, and scans it:<ul style="list-style-type: none">◆ If the response is safe, it is downloaded to the browser◆ If the response is a threat, a Block Page message is sent to the browser■ By default, the Inspect action will terminate SSL traffic if your policy allows it. This action can be performed without content analysis and download scanning. In this case, it will only terminate SSL traffic	<ul style="list-style-type: none">■ See section 4.3.4.2 "Document Isolation Viewer" for information about supported file sanitizers■ See section 4.4.6 "Creating Custom Pages" for information about the Block Page object■ See the section Limited Inspect Action, below, for instructions on how to disable content analysis and download scanning in the Inspect action
Pass	<ul style="list-style-type: none">■ The security level is the lowest. This action is used only if the website is trusted 100%■ The Threat Isolation Proxy passes web content directly between the endpoint browser and the web application■ No scanning or isolation process takes place■ The Pass action does not terminate SSL traffic	



Action	Description	For More Information
Block	<ul style="list-style-type: none">■ The security level is the strictest. WebSocket requests of this type are considered dangerous or illegitimate, and are blocked from being viewed■ The Symantec Threat Isolation Platform checks the WebSocket request and prevents access to the destination website■ The Symantec Threat Isolation Platform notifies the endpoint browser via a block page that the request has been blocked■ A webpage can include iFrames that can also be blocked. The end user sees only the parts of the page that are not blocked	See section 4.4.6 "Creating Custom Pages" for information about the Block Page object

Action	Description	For More Information
Isolate	<ul style="list-style-type: none">■ The security level is high; HTTP/S responses of this type are always isolated■ The Symantec Threat Isolation Platform checks the WebSocket request and determines that it should be isolated■ The Symantec Threat Isolation Platform translates website content into visible elements and collects user gestures to the isolated virtual browser in the TIE■ The Symantec Threat Isolation Platform isolates the HTTP/S response and sends it to the endpoint browser for display■ The Isolate action requires designation of both a Download Profile and an Upload Profile	<ul style="list-style-type: none">■ See section 4.3.4 "Defining Download Profiles"■ See section 4.3.5 "Defining Upload Profiles"



Action	Description	For More Information
Inspect	<ul style="list-style-type: none">■ The security level is medium. WebSocket requests of this type are considered neutral■ The action is Inspect only if the downloaded content includes links to downloaded files■ The Inspect action requires definition of a Download Profile■ The Symantec Threat Isolation Platform downloads the HTTP/S response to the server, inspects it, and scans it:<ul style="list-style-type: none">◆ If the response is safe, it is downloaded to the browser◆ If the response is a threat, a Block Page message is sent to the browser■ By default, the Inspect action will terminate SSL traffic if your policy allows it. This action can be performed without content analysis and download scanning. In this case, it will only terminate SSL traffic	<ul style="list-style-type: none">■ See section 4.3.4.2 "Document Isolation Viewer" for information about supported file sanitizers■ See section 4.4.6 "Creating Custom Pages" for information about the Block Page object■ See the section Limited Inspect Action, below, for instructions on how to disable content analysis and download scanning in the Inspect action
Pass	<ul style="list-style-type: none">■ The security level is the lowest. This action is used only if the website is trusted 100%■ The Threat Isolation Proxy passes web content directly between the endpoint browser and the web application■ No scanning or isolation process takes place■ The Pass action does not terminate SSL traffic	
Block	<ul style="list-style-type: none">■ The security level is the strictest. WebSocket requests of this type are considered dangerous or illegitimate, and are blocked from being viewed■ The Symantec Threat Isolation Platform checks the WebSocket request and prevents access to the destination website■ The Symantec Threat Isolation Platform notifies the endpoint browser via a block page that the request has been blocked■ A webpage can include iFrames that can also be blocked. The end user sees only the parts of the page that are not blocked	See section 4.4.6 "Creating Custom Pages" for information about the Block Page object



Limited Inspect Action

As explained in section [4.2.7.2 "Rule Actions"](#), the Inspect action terminates SSL traffic (if your policy allows it) as well as performs content analysis and download scanning. However, your organization might want to terminate SSL traffic without also performing content analysis and download scanning, for reasons of privacy. For this scenario, you can disable the Inspect action's content analysis and download scanning capabilities in the Rule Advanced Settings so that the Inspect action will only terminate SSL traffic.

To exclude content analysis and download scanning from the Inspect action:

1. Go to:
`Rule Advanced Settings > Internal Settings`
2. Clear the checkbox for the parameter `proxy.enable_content_scanning` to disable it. For more information, see section [4.4.10 "Creating Rule Advanced Settings"](#).

Selective Isolation in Online Service Suites

Your organization might decide to isolate some, but not all, online services included in Microsoft Office 365, G Suite and other online service suites. For example, if you are using Microsoft Office 365, your organization might decide to isolate only Outlook while bypassing all other services included in that suite.

To be able to use a suite's services, you must authenticate with its login service. If you want to isolate only some of its services while bypassing others, this means that Symantec Threat Isolation must sometimes isolate the suite's anchor URLs used for authentication, while at other times bypassing them.

The Selective Isolation mode enables you to isolate specific services while bypassing all others included in an online service suite. Symantec Threat Isolation dynamically detects the anchor URLs that are used for authentication and bases its decision of whether to isolate or bypass them on the context of the session.

For example, if according to your policy only webmail sites must be isolated, and you access a Gmail account from an isolated browsing session, Symantec Threat Isolation will isolate the Google account's login page. If you access Google Docs, which according to your policy is not isolated, then the Google account's login page will not be isolated.

To enable selective isolation of services within online service suites:

1. Go to:
`Policy Entities → Policy Advanced Settings → Internal Settings`
2. Select the checkbox for the parameter `coupled_urls_isolation_stickiness`.

**Note**

It is recommended to contact Symantec Threat Isolation technical support for assistance with internal settings.

4.3 Defining Profiles

As a Management user, you need to define various types of profiles. These profiles specify the actions that Symantec Threat Isolation will apply when a policy rule is matched.

You can define the following profiles:

- Isolation Profile – Defines the browsing settings that will be applied to HTTP/S responses. See section [4.3.3 "Defining Isolation Profiles"](#).
- Download Profile– Defines the download settings that will be applied to download file requests from the end user. See section [4.3.4 "Defining Download Profiles"](#).
- Upload Profile – Defines upload settings that will be applied to upload file requests from end users. See section [4.3.5 "Defining Upload Profiles"](#).
- Activity Log Profile – Defines the types of end-user activities that will be logged by Symantec Threat Isolation Management. See section [4.3.6 "Defining Activity Log Profiles"](#).
- End-User Data Protection Profile – Defines settings that will be applied to end users to prevent them from submitting sensitive data to potentially malicious websites. See section [4.3.7 "Defining End-User Data Protection Profiles"](#).
- Application Data Protection Profile – Defines activity settings that will be applied to end users to protect your organization's applications by controlling how information can leave the application, for example via copying or printing. See section [4.3.8 "Defining Application Data Protection Profiles"](#).
- Anti-Bot Protection Profile – Defines settings that will be applied to prevent bots inside the organization's network from reaching the Internet using the HTTP protocol. See section [4.3.9 "Defining Anti-Bot Protection Profiles"](#).



4.3.1 Accessing Profiles

1. To access the list of profiles, go to:
Profiles → [List of Profiles]
2. Select the relevant profile.

The following sections describe how to define each profile type.

4.3.2 Cloning Objects

Cloning allows you to conveniently recreate profiles and Gateway Advanced Settings. For example, this is useful if you want to fine-tune Gateway Advanced Settings or modify one or more rules in an existing profile. Rather than having to create a new object and configure it to match the existing one, you can simply recreate and adapt the existing object.

1. In the grid of the object that you want to clone, click this icon:



2. Click Create Copy.
A copy of the original object is displayed, with a different name (for example, "MyProfile_copy").
 3. Modify the new object according to your requirements, and then click Create.
-

4.3.3 Defining Isolation Profiles

4.3.3.1 Overview

Isolation Profiles define the browsing settings that Symantec Threat Isolation will apply to HTTP/S responses. The isolation mode that you configure determines how isolated content will be rendered to end users in your organization. Both isolation modes are highly secure, and suitable for endpoint as well as web application protection topologies. The considerations below will help you determine the best isolation mode for your organization.

Grid Rendering Mode (GRM)	Vector Rendering Mode (VRM)
■ Compatible for all websites	■ Compatible for all websites



Grid Rendering Mode (GRM)	Vector Rendering Mode (VRM)
■ Displays the browser content as images. Hides DOM elements, CSS, internal logic and API calls from the client	■ Displays HTML visual elements (DOM elements and CSS). Hides internal logic and API calls from the client
■ Utilizes high bandwidth	■ Utilizes lower bandwidth
■ Utilizes high gateway Memory and CPU usage	■ Utilizes lower gateway Memory and CPU usage

4.3.3.2 Adding an Isolation Profile

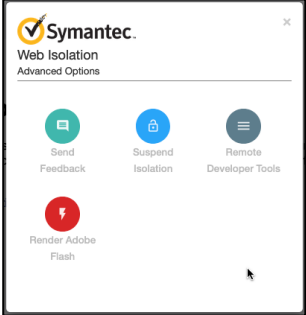
1. To access the Isolation Profiles page, go to:
Profiles → Isolation Profiles
2. Add a new Isolation Profile by clicking New Isolation Profile, or by cloning an existing Isolation Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the following table for the new profile, and then click Create.

Parameter	Description	For More Information
General		
Isolation Mode	<ul style="list-style-type: none">■ Grid Rendering - Displays the browser content to the client as images. The DOM elements, CSS, internal logic and API calls never reach the client. This mode is recommended in the Web Application Isolation Gateway Mode topology, for application protection■ Vector Rendering - Displays the browser content to the client as HTML visual elements composed of alternate DOM and CSS content. The internal logic and API calls (JavaScript) never reach the client	See section 4.3.3 "Defining Isolation Profiles"
Vector Rendering Settings (displayed only in Vector Rendering Mode)		



Parameter	Description	For More Information
Grid Rendering URLs	<ul style="list-style-type: none">■ Use Symantec's dynamically-updated list of URLs■ Use a customized list of URLs. <p>Specify grid rendering destinations - Enables you to add websites that display better in GRM than in VRM to a customized list of URLs for Grid Rendering. The Threat Isolation Gateway reads this Grid Rendering Destinations list, and if the website is included in it, it will be rendered in GRM. It is good practice to report such websites to Symantec Threat Isolation technical support</p> <p>NOTE: In the activity logs, the Rendering Mode shows the actual website rendering mode. For the reason explained above, the actual rendering mode might be GRM even though the configured Isolation mode is VRM</p>	



Parameter	Description	For More Information
Context Menu	<p>Context menu to display in isolated pages:</p> <ul style="list-style-type: none">■ Symantec's custom context menu■ The browser's native menu (default) <p>NOTES:</p> <ul style="list-style-type: none">■ Symantec's custom context menu is always displayed in the following cases:<ul style="list-style-type: none">◆ On "contenteditable elements" in IE and Edge browsers◆ When "Save image as" and/or "Save link as" were not selected in the Application Data Protection Profile settings. In this case, the end user cannot perform the actions. Therefore, the custom context menu hides them.■ Regardless of which context menu is selected, the end user can display an Advanced Options screen by pressing Ctrl+Q. This screen contains the options that are specific to Symantec Threat Isolation.  <ul style="list-style-type: none">◆ Send Feedback - Allows the end user to send feedback about any isolated or blocked webpage◆ Suspend Isolation - Allows the end user to open the same webpage without isolation for the configured period of time◆ Remote Developer Tools - Opens a new tab that launches the remote Developer Tools◆ Render Adobe Flash - Enables the	<p>See section 4.3.8.2 "Adding an Application Data Protection Profile"</p> <ul style="list-style-type: none">■ For Send Feedback, see section 4.7.8 "Defining Gateway Advanced Settings" and section 8.1.5 "Send Feedback"■ For Suspend Isolation, see section 4.4.10 "Creating Rule Advanced Settings"■ For Remote Developer Tools, see section 4.3.8.2 "Adding an Application Data Protection Profile" 4.3.8.3 "Opening Developer Tools Remotely"■ For Adobe Flash, see section 8.1.4 "Render Adobe Flash"



Parameter	Description	For More Information
	Adobe Flash plug-in. Available only when Symantec Threat Isolation does not automatically enable Flash rendering in the browsed website. Note that these menu options are available only when they are allowed by your policy.	
Grid Rendering Settings		
These settings also affect HTML elements that are used to draw graphics on a web page. Note that higher quality images use more bandwidth, which might cause latency issues		
Compression	For isolated content, defines the type of compression	
WebP Support	Select to use WebP image compression format with compatible browsers	
Image Quality	Values range from 0-100, where 95 and above represent excellent quality. Note that higher quality settings impact the required bandwidth.	
Frame Rate	Defines the number of frames per second for the isolation refresh rate	
Scroll Quality	Select to adjust image quality during scroll	
Video Frame Rate	For HTML video elements requiring isolation, defines the number of frames per second	
Media Quality		
(Relevant to VRM and GRM) Enforces the maximum media quality the end user can consume, to limit bandwidth utilization.		
Video Resolution	Select to enforce the selected maximum video resolution NOTE: Enforceable only when the media provider allows the video resolution to be controlled	



Parameter	Description	For More Information
Image Quality	<ul style="list-style-type: none">■ Select to enforce image compression■ When Enforce image compression is selected, you can use the JPEG image quality slider to adjust the JPEG compression level. By default, it is set to 80 on scale of 1-80 (80 meaning that the original file size is kept). A lower compression level reduces the image quality, but saves bandwidth	
Audio Quality	<ul style="list-style-type: none">■ Select to activate audio compression.■ When Enforce audio compression is selected, the original audio file is compressed to save bandwidth. Compression does not affect audio file quality. This setting applies only to audio files and not to the audio in video files.<ul style="list-style-type: none">◆ To further compress the audio file and reduce bandwidth consumption, select Convert to a single channel (mono). NOTE: Converting stereo files to mono files may result in loss of audio quality.	
Miscellaneous		
Print	Select to neutralize exploits in printed webpages (relevant only to GRM)	
Isolation Indication	<p>Select to display a graphic mark around the body of a webpage to indicate that the site is isolated. The Indication Color drop-down list allows you to select the color of the indicator: red, blue, green, or a custom hex color you can define using a color picker</p> <p>NOTE: To display the indicator in all isolated websites, you must select this parameter for each isolation profile individually</p>	



4.3.4 Defining Download Profiles

4.3.4.1 Overview

Download Profiles define the download settings that Symantec Threat Isolation will apply to file-download requests from the end user. You can configure how Symantec Threat Isolation will handle file downloads depending on the type of the file (for example, Microsoft PowerPoint).

Download Profile Actions

The table below describes the Download Profile actions that can be enforced for each file type. Symantec Threat Isolation provides a fairly secure out-of-the-box default download setting per file type. In general, the default download settings per file type can be used and no changes are necessary.

Action	Description	For More Information
Allow	<ul style="list-style-type: none">■ Security level is lowest; files of this type are considered safe■ The Symantec Threat Isolation Platform checks the file type (by the file extension and MIME type) and determines that its handling type is Allow■ The Symantec Threat Isolation Platform downloads the file to the server, inspects it, to confirm its file type, and downloads it to the browser <p>NOTE: The download UI element viewed by the client is similar to the browser's regular UI, but it is actually part of Symantec Threat Isolation</p>	



Action	Description	For More Information
Scan	<ul style="list-style-type: none">■ Security level is medium; files of this type are considered neutral■ The Symantec Threat Isolation Platform checks the file type (by the file extension and MIME type) and determines that its handling type is Scan■ The Symantec Threat Isolation Platform downloads the file to the server, inspects it, and scans it.<ul style="list-style-type: none">◆ If the file is safe, it is downloaded to the browser◆ If the file poses a threat, a Block Page message is sent to the browser <p>NOTE: The Scan action is applied to image file types (bmp, gif, jfif, x-png, tiff, ico) only when the end user tries to download the image. It is not applied when an image is copied or saved using context menu options in an isolated website, because when these options are available, the image has been sanitized and resides on the endpoint machine</p>	<p>See section 4.3.4.2 "Document Isolation Viewer" for details of the supported file sanitizers</p> <p>See section 4.4.6 "Creating Custom Pages" for a description of the Block Page object</p>
Block	<ul style="list-style-type: none">■ Security level is highest; files of this type are considered dangerous.■ The Symantec Threat Isolation Platform checks the file type (by the file extension and MIME type) and determines that its handling type is Block■ The file is not downloaded to the server, and a Block Page message is sent to the endpoint browser <p>NOTE: The Block action is applied to image file types (bmp, gif, jfif, x-png, tiff, ico) only when the end user tries to download the image. It is not applied when an image is copied or saved using context menu options in an isolated website, because when these options are available, the image has been sanitized and resides on the endpoint machine</p>	<p>See section 4.4.6 "Creating Custom Pages" for a description of the Block Page object</p>
View	<ul style="list-style-type: none">■ The file is viewed in the endpoint browser using the Symantec Threat Isolation Document Isolation viewer, but is not saved to the endpoint's operating system. This is similar to the way PDF files are often viewed in browsers <p>NOTE: The View action is limited to document files, such as MS PowerPoint, Word, Excel, PDF, XML Paper Specification (XPS) files, Visio, AutoCAD.</p>	<p>See section 4.3.4.2 "Document Isolation Viewer"</p>



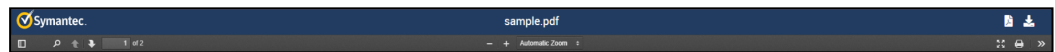
4.3.4.2 Document Isolation Viewer

Download file types with a View action are isolated and presented to the end user in the Document Isolation Viewer.

This can be done in two different ways:

- Using Symantec Threat Isolation's Cloud Document Isolation Server (default).
- Using an on-premises Document Isolation Server. For information about installing and using an on-premises Document Isolation Server, see the section ["Using an On-Premises Document Isolation Server"](#), below.

The Document Isolation Viewer displays the isolated file with the following header:



The end user can select one of the following actions:

- Download the scanned document
- Download the document as a PDF
- Print the document
- Select and copy parts of the document

You can hide one or more of the above options using the `fileViewer.disableDownload`, `fileViewer.disablePrintButton`, `fileViewer.disableCopy`, or `fileViewer.disablePdfDownload` settings in Download Profile Advanced Settings.

You can also change the header displayed for the document using the `fileViewer.displayName` setting in Download Profile Advanced Settings.

Note that the file will be downloaded from the Document Isolation Viewer only if the policy rule "Document Isolation Download Rule" is active (by default, it is inactive).

Using an On-Premises Document Isolation Server

Download file types that are designated as View are isolated and shown to the end user in the Document Isolation Viewer. By default, this process is handled by Symantec Threat Isolation's Cloud Document Isolation Server; the files are sent to the Cloud encrypted and are removed when the specified timeout expires.

However, if your organization prefers to keep the contents of its files on-premises, you can choose to use an on-premises Document Isolation Server. Upon your



request, Symantec will provide a Document Isolation Server installation zip file and an On-Premises Document Isolation Server Installation Guide with instructions for installing and defining the server.

Opening Documents in New Tab in Document Isolation Viewer

When the end user clicks on a link from a webpage to a document of a file type with a View action, the document is viewed in the browser using the Document Isolation Viewer. By default, the document is opened in the same tab on top of the webpage that contained the link. You can change the default Advanced Setting, so that documents that are viewed using the Document Isolation Viewer will be opened in a new tab. For more information, see section [4.3.4.5 "Defining Download Profiles Advanced Settings"](#).

4.3.4.3 Downloading Files Safely

Symantec Threat Isolation offers a major advantage when files need to be downloaded. The files are fully downloaded to the Symantec Threat Isolation Platform and can be sanitized or modified before the download connection to the endpoint browser is initiated.

This allows Symantec Threat Isolation to integrate multiple possible solutions for downloads:

- Sanitizing files such as PDF or Microsoft Office files by creating new “known good” files, and then importing text and images from the original document into the “known good” document and having the resulting document sent to the endpoint browser
- Sending files to a sandbox for analysis and waiting for a response prior to sending the file to the end user who can, in the meantime, view the content on the Symantec Threat Isolation Platform
- Scanning the file with multiple detection engines, using threat intelligence services
- Storing the files in a queue for manual review

The Symantec Threat Isolation Platform is currently integrated with a number of third-party file sanitizing tools. File sanitizers are grouped according to their method of sanitization.



Symantec Threat Isolation supports the following file sanitizers out of the box:

Type	File Sanitizer
Sandbox	<ul style="list-style-type: none">■ Checkpoint Sandblast Zero-Day Protection■ Palo Alto Networks WildFire■ Symantec Cynic
Anti-Malware	<ul style="list-style-type: none">■ Symantec AV. For more information, see the section "Symantec AV (Anti-Virus)" below this table■ Integrated Antivirus - No license required■ OPSWAT Metadefender Cloud■ Virus Total
Threat Feed	<ul style="list-style-type: none">■ Google Safe Browsing
Content Disarming	<ul style="list-style-type: none">■ Votiro SDS API 3.0■ OPSWAT Metadefender Core■ YazamTech SelectorIT - To integrate this file sanitizer, contact Symantec Threat Isolation technical support

Note that most of the supported file sanitizers require a license. Their license information must be taken from the external system and specified in the Download Profile > Advanced Settings. In the case of Symantec AV, a Symantec product, the license information is taken automatically from the Symantec Network Protection Licensing Portal (NPLP) (for more information, see section [3.5.7 "Defining the Management Gateway"](#), step 11) and loaded to the Symantec Threat Isolation Platform.

Contact Symantec Threat Isolation technical support for assistance in selecting the file sanitizer that best suits your organization, or if you want to add additional sanitizers.

Symantec AV (Anti-Virus)

Symantec AV is a Symantec anti-malware file sanitizer that provides a range of advanced threat-defense capabilities, including machine learning-powered security. Since Symantec AV is a Symantec product, it can be conveniently integrated with the Symantec Threat Isolation Platform. You activate the sanitizer by checking the Symantec AV checkbox in the Downloads Profile. Once you have configured its license, no additional advanced settings need to be configured, as is necessary when using a file sanitizer from any other vendor. For information about registering licensed components, see section [4.20.1 "Registering your Licensed Components"](#).

4.3.4.4 Adding a Download Profile

1. To access the Download Profiles page, go to:

Profiles → Download Profiles




2. Add a new Download Profile by clicking New Download Profile or by cloning an existing Download Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the table below for the new profile, and then click Create. Note that the Create Download Profile window includes two tabs: General and File Types.

Parameter	Description	For More Information
General		
File Sanitizers	<ul style="list-style-type: none">■ Sanitizers used for scanning file types associated with this Download Profile■ When using the Symantec Cynic sandboxing system, select Symantec Cynic under File Sanitizers/Sandbox and then select the Cynic Server Setting from the drop-down list	<p>See section 4.3.4.2 "Document Isolation Viewer" for a description of file sanitizers</p> <p>See section 4.17 "Configuring Cynic Server Settings"</p>
Max Download Size (MB)	<ul style="list-style-type: none">■ Maximum download size, in MBs■ If the size of the file for download exceeds Max Download Size, the file will not be downloaded and a message will be sent to the end user	
Archive Options	<p>How archived files will be handled:</p> <ul style="list-style-type: none">■ Enforce policy on archive files - Extracts files and enforces policy on each file type. If one file type is blocked, the entire archive file will be blocked■ Block archives that failed extraction - Blocks all archive files that failed to extract <p>If files do not extract properly, default policy is to pass the entire archive file to the end user</p> <p>If no archive options are checked, the policy set for the specific archive file type will be followed</p>	



Parameter	Description	For More Information
Password Protected Archives	How password-protected archives will be handled: <ul style="list-style-type: none">■ Process without file extraction (default)■ Request passwords and extract files■ Block password-protected archives	
Document Isolation Type	Which server to use for showing “View” download file types in the Document Isolation Viewer: <ul style="list-style-type: none">■ Cloud - The Cloud Document Isolation Server■ On-Premises - An on-premises Document Isolation Server. Specify the address of the on-premises Document Isolation Server in the following format: https://<document-isolation-host> It is recommended to use the DNS name of the server rather than its IP address. NOTE: The on-premises Document Isolation Server must be accessible by the Threat Isolation Engine (TIE)s. Its server certificate must be added to the Trusted Certificates	See section 4.3.4.2 "Document Isolation Viewer"
Advanced Settings	Click EDIT to open Advanced Settings parameters related to: <ul style="list-style-type: none">■ Inspect Mode■ File Sanitizers■ Archive Files■ Viewer Settings■ Miscellaneous Download Advanced Settings NOTE: Contact Symantec Threat Isolation technical support for assistance with these settings	See section 4.3.4.5 "Defining Download Profiles Advanced Settings"
File Types		
+ADD TYPE button	Enables adding a new file type. When adding a new file type, specify the following: <ul style="list-style-type: none">■ Name - Name of the file type■ Extensions - Extensions by which the file type is recognized■ Policy - Download policy actions	See section 4.3.4.1 "Overview"



Parameter	Description	For More Information
Search	Enables searching for a specific file type	
	<p>Provides a list of global actions that can be applied to all file types in the list:</p> <ul style="list-style-type: none">■ View All Documents - All documents are presented to the end user in the Document Isolation Viewer■ Scan All - Scans all files of this type■ Allow All - Allows download without scanning for all files of this type■ Block All - Blocks all files of this type from download■ System Defaults - Values defined out of the box	See section 4.3.4.2 "Document Isolation Viewer" for a description of the Symantec Threat Isolation Document Isolation Viewer
Unknown Type	Defines Download Profile action for unknown file types	
Inspect Advanced Settings	Click EDIT to view the Inspect Advanced Settings dialog (explained below)	

The Inspect advanced settings, explained in the following table, are relevant only when the Inspect verdict is reached: Either when rules with Inspect action are matched, or through website subresources policy:



Parameter	Description	For More Information
Content Scanning Criteria	<p>Enables selecting criteria for excluding content from scanning when the Inspect verdict is reached, either when rules with Inspect action are matched, or through website subresources policy</p> <p>Whitelisting URLs and file types is useful for the following reasons:</p> <ul style="list-style-type: none">■ Efficiency - Avoids latency as a result of image scanning■ Connectivity - Avoids video files being blocked when the end user skips to the middle of the file during streaming. When this is done, Symantec Threat Isolation is unable to identify the file type and therefore labels it as "Unknown." If the download policy calls for blocking Unknown file types, the video will be blocked. This scenario is avoided by whitelisting, for example, MP3 file types <p>The following whitelisting options are available:</p> <ul style="list-style-type: none">■ Exclude by a customized list of URLs - The Content-Scanning Whitelisted Destinations object allows you to define the URLs of all content to be excluded from scanning. NOTE: All Download Profiles refer to this same object. The object can be defined only from this location■ Exclude by content type - An editable, comma-separated whitelist of content types to be excluded from scanning	<p>See section 4.4.10 "Creating Rule Advanced Settings", Websites Subresources Policy section</p>
Unknown File Type Policy	<p>The unknown file type policy:</p> <ul style="list-style-type: none">■ Allow - The file is downloaded and considered safe■ Scan (default) - The file is scanned.■ Block - The file is blocked <p>NOTE: Some websites download certain media files in chunks. Symantec Threat Isolation is unable to identify the file type of these chunks and therefore labels them as "Unknown." If your unknown file type policy is Block, the media file chunks will be blocked. This might cause connectivity issues</p>	<p>See section 4.3.4 "Defining Download Profiles"</p> <p>See section 4.4.10 "Creating Rule Advanced Settings", Websites Subresources Policy section</p>



4.3.4.5 Defining Download Profiles Advanced Settings

- To configure Download Profile Advanced Settings, go to:
Profiles → Download Profiles → Advanced Settings

Configuring File Sanitizer Settings per Download Profile

You can configure File Sanitizer settings per Download Profile. This is useful in case of multiple Download Profiles with different sanitizer requirements.

- In Download Profile Advanced Settings, search for the required sanitizer and modify its settings according to your requirements.

Note

File Sanitizer settings are not global. This means that when you add a new Download Profile, you must remember any overrides to the File Sanitizer settings and sync them. Therefore, it is good practice to clone a Download Profile object and then modify the File Sanitizer settings.

Configuring Symantec Cynic Scanning Mode for a Download Profile

You can set the Symantec Cynic scanning mode for a specific Download Profile. For this particular Download Profile, this setting overrides the default scanning mode configured in the Cynic Server Settings.

1. In Download Profile Advanced Settings, search for cynic.api.scanningMode.
2. Select the scanning mode from the drop-down list:
 - ◆ Default Value - The policy as set in the Cynic Server Settings. Note that all Download Profiles for which this scanning mode is selected will be affected when the default scanning mode is changed in the Cynic Server Settings.
 - ◆ Hold - This setting overrides the default scanning mode configured in the Cynic Server Settings, for this specific Download Profile.
 - ◆ Background - This setting overrides the default scanning mode configured in the Cynic Server Settings, for this specific Download Profile.

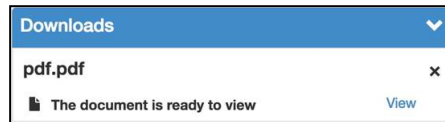
Opening Documents in New Tab in Document Isolation Viewer

You can change the default Advanced Setting so that documents that are viewed using the Document Isolation Viewer will be opened in a new tab.



- In Download Profile Advanced Settings, search for `viewDocumentInNewTab` and select the checkbox (True).

Now, when the end user clicks on the link, the following pop-up message appears in the endpoint browser:



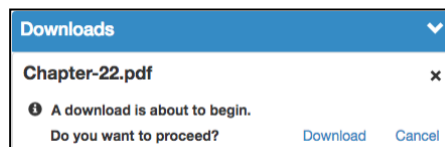
When the end user clicks View, the document opens in a new tab and is viewed using the Document Isolation Viewer.

Prompting the End User Before File Download

You can display a prompt in the endpoint browser before a file download begins. The prompt informs the end user that a download is about to start and asks for confirmation. Prompting before downloading prevents files from being downloaded without the end user's consent (as occurs, for example, in drive-by download attacks).

- In Download Profile Advanced Settings, search for `fileDownloadPrompt` and select the checkbox (True).

Once enabled, the following prompt appears in the endpoint browser before a download begins:



4.3.5 Defining Upload Profiles

4.3.5.1 Overview

Upload Profiles define upload settings that Symantec Threat Isolation will apply to file-upload requests from the end user. You can configure how Symantec Threat Isolation will handle file uploads depending on the type of the file.

Upload Profile Actions

The table below describes the Upload Profile actions that can be enforced for each file type.



Action	Server Handling	For More Information
Allow	<ul style="list-style-type: none">■ Security level is lowest; files of this type are considered safe■ The Symantec Threat Isolation Platform uploads the file to the server, inspects it to confirm its file type, and transmits it	
Block	<ul style="list-style-type: none">■ The file is not permitted for upload■ A Blocked File message is sent to the browser	See section 4.4.6 "Creating Custom Pages" for Block Page entity
Scan	<ul style="list-style-type: none">■ Scan the file to be uploaded for the purpose of Data Leakage Prevention (DLP)	See section 4.18 "Configuring Data Leakage Prevention Server Settings"

4.3.5.2 Adding an Upload Profile


1. To access the Upload Profiles page, go to:
Profiles → Upload Profiles
2. Add a new upload profile by clicking New Upload Profile, or by cloning an existing Upload Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the table below for the new profile, and then click Create. Note that the Create Upload Profile window includes two tabs: General and File Types.

Parameter	Description	For More Information
General		
Max Upload Size (MB)	<ul style="list-style-type: none">■ Maximum upload size in MBs■ If size of file for upload exceeds Max Download Size, file is not uploaded and message is sent to the end user	
Fail Open Policy	Enables scanning to be skipped and uploading to proceed in case of a failure during the scanning process. Relevant for both files and network requests	
Scan Settings		
Enable scanning	Select to enable file scanning	



Parameter	Description	For More Information
Data Leakage Prevention Server Settings	Select the relevant Data Leakage Prevention Server Settings from the drop-down list	See section 4.18 "Configuring Data Leakage Prevention Server Settings" See section 8.4 "Data Leakage Prevention"
Max Scan Size (MB)	Specify the maximum scan size, in MB. Relevant for both files and network requests. Default: 30 MB. Maximum upload size (input): 1.5 GB	
Oversized Content Policy	Select the action to be performed when the maximum scan size is exceeded: <ul style="list-style-type: none">■ Allow (default) - If the content should be scanned but its size exceeds the configured maximum scan size, the upload will be allowed but the content will not be scanned■ Block - If the content should be scanned but its size exceeds the configured maximum scan size, the upload will be blocked. The content will not be scanned	
File Scanning Timeout (sec)	Specify the timeout. If scanning takes more than the specified number of seconds, it will fail. In that case, file scanning will be skipped and the file will be uploaded if Fail Open Policy is selected	
Monitor Only Mode	Only log the scan result - When selected, content that should be blocked according to the DLP scan verdict will not be blocked, but the scan verdict will appear in the activity log	
Network Requests		
Scan network request data	Select to scan network request data Click EDIT to view the Network Request Scanning Settings dialog (explained below)	
File Types		



Parameter	Description	For More Information
+ADD TYPE button	Enables adding a new file type. When adding a new file type, specify the following in the Create File Type dialog, and then click Create: <ul style="list-style-type: none">■ Name - Name of the new file type■ Extensions - Extensions by which the file type is recognized■ Default Policy - Default upload policy action	See section 4.3.5.1 "Overview"
Search	Enables searching for specific file type	
Unknown Type	Defines upload profile action for unknown file types	
	Provides a list of global actions that can be applied to all file types in the list: <ul style="list-style-type: none">■ Allow All - Allow all file uploads■ Block All - Block all file uploads■ Scan All - Scan all file uploads■ System Defaults - Values defined out of the box	
Inspect Advanced Settings	Click EDIT to view the Inspect Advanced Settings dialog (explained below)	

The following advanced settings are relevant only when the Inspect verdict is reached (either when rules with an Inspect action are matched, or through the website subresources policy):

Unknown File Type Policy	Select the unknown file type policy: <ul style="list-style-type: none">■ Allow (default) - The file is uploaded and considered safe■ Scan - The file is scanned■ Block - The file is blocked	See section 4.3.5 "Defining Upload Profiles"
--------------------------	--	--

In the Network Request Scanning Settings dialog, configure the parameters described in the table below:

Parameter	Description	For More Information
Scan Settings		



Scanning Timeout (sec)	Specify the timeout. If scanning takes more than the specified number of seconds, it will fail. In that case, network request data scanning will be skipped and the data will be uploaded, if Fail Open Policy is selected	
Minimal Scanning Size (KB)	<p>Specify the minimum scanning size for network requests. Default: 4 KB</p> <ul style="list-style-type: none">■ If the scanning size is less than the specified value, the network request will not be scanned (meaning it will be allowed)■ If set to 0, all network requests with a size of up to Max Scan Size will be scanned	
End User Notifications		
Mode	<p>When a top-level navigation resource and/or a subresource is blocked because Symantec Data Loss Prevention criteria were matched with a Block action, the end user is notified via a Data Leakage Prevention pop-up message. Select one of the following options to notify the end user when a resource is blocked:</p> <ul style="list-style-type: none">■ Notify only for top-level navigation■ Notify for both top-level navigation and sub-resources (default)	See section 8.4 "Data Leakage Prevention"

4.3.6 Defining Activity Log Profiles

4.3.6.1 Overview

Activity Log Profiles define the types of end-user activities that Symantec Threat Isolation Management will log in the activity logs.

4.3.6.2 Adding an Activity Log Profile

1. To access the Activity Log Profiles page, go to:
Profiles → Activity Log Profiles
2. Add a new Activity Log Profile by clicking New Activity Log Profile, or by cloning an existing Activity Log Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the table below for the new profile, and then click Create.



Parameter	Description	For More Information
General		
Active	Enables or disables logging of all activities listed in this table	
Logging Criteria		
Network Events		
Top-level navigation	Logs end-user navigation to websites, but not depth lower than first level (i.e., the URL that appears in the browser bar)	
Network requests	<ul style="list-style-type: none">■ Logs all resource requests associated with a webpage, including origins of all elements presented on the page■ Enables you to track all elements in the webpage (for example, countries, sites, and so on)■ Enables you to track the source of malware that associated with a webpage	
Network statistics	Adds a logging row with an event named Session End. Additional statistics are logged for the session	
Forward to isolation	Logs an event when the proxy matches a rule with the Isolate action	
Downloaded Files	Logs an event when a file is downloaded	
Uploaded Files	Logs an event when a file is uploaded	
Flash element loaded	Logs an event when a Flash element was loaded on the server and has been isolated	
Website authentication	Logs an event when a website returns an HTTP authentication response, prompting the end user to fill in their credentials	
URL Intelligence		
Always log categories	Logs the category of the accessed website (i.e., iFrames, images, and other resources) NOTE: Logging categories impacts performance	



Parameter	Description	For More Information
Always log risk level	Logs the risk level NOTE: Logging the risk level impacts performance	
User Gestures		
Keyboard and mouse events	Keyboard text content - Logs any key presses on the end user's keyboard, and tracks mouse clicks	
Clipboard events	<ul style="list-style-type: none">■ Copied content - Logs end-user data copied to clipboard■ Pasted content - Logs end-user data pasted from clipboard	
Downloaded File Hash Computation		
MD5	The MD5 signature of the downloaded file	
SHA1	The SHA1 hash value of the downloaded file	
SHA256	The SHA256 hash value of the downloaded file	

4.3.6.3 URL Query Parameter Privacy

By default, URL query parameters are not logged but rather saved with an asterisk (*) to ensure privacy of the query. If the URL query parameters must be reported in the log, and it is permitted by state regulations, you can change the advanced parameter using the System Configuration > Advanced Configuration menu option.

To report the URL query parameters, change the value of the following parameter from false to true:

```
activityLogConfiguration.logUrlQueryParams
```

IMPORTANT!

Changing the Advanced Settings might result in unexpected system behavior and should only be done in consultation with Symantec Threat Isolation technical support.



4.3.7 Defining End-User Data Protection Profiles

4.3.7.1 Overview

End-User Data Protection Profiles define settings that protect end users from potentially malicious websites by preventing them from submitting sensitive data to such sites. Symantec Threat Isolation provides an End-User Data Protection Profile out of the box. You can add additional End-User Data Protection Profiles, with restricted privileges that you can assign to individual end users or to end user groups.

4.3.7.2 Adding an End-User Data Protection Profile

1. To access the End-User Data Protection Profiles page, go to:
`Profiles → End-User Data Protection`
2. Add a new End-User Data Protection Profile by clicking New End-User Data Protection, or by cloning an existing End-User Data Protection Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the table below for the new profile, and then click Create.

Parameter	Description	For More Information
Anti-Phishing		
The options in this subsection refer to the verdict. You need to specify the match criteria for the policy rule (for example, phishing websites, high-risk websites, and so on)		See section 4.4 "Defining Policy Entities"
Read-Only Page	<ul style="list-style-type: none">■ Prevent the end user from entering data - Disables all input fields when a website might be unsafe. The Page option allows you to customize the read-only page dialog■ Allow end user to override this protection - Allows the end user to override this extra protection. In this case, a warning will be displayed	See section 4.4.6.2 "Creating a Custom Read-Only Page"



Parameter	Description	For More Information
Sensitive Data Protection	<ul style="list-style-type: none">■ Prevent submission of sensitive data over an insecure connection - Disables input fields when a website is unsafe■ Allow end user to override this protection - Allows the end user to override this extra protection. In this case, a warning is displayed	
Permissions		
Clipboard	<ul style="list-style-type: none">■ Paste - Enables pasting copied data from the clipboard to the webpage using the keyboard or the right-click menu.<ul style="list-style-type: none">◆ Include HTML content - Allows rich text to be pasted to the webpage. If this checkbox is clear, rich text in the clipboard will be pasted as unformatted text◆ Include images - Allows images to be pasted to the webpage. If this checkbox is clear, no images will be pasted	

4.3.8 Defining Application Data Protection Profiles

4.3.8.1 Overview

Application Data Protection Profiles define settings that protect an organization's application data by controlling how information can leave the application. These settings define what end users are allowed to do with the applications they view. For example, copying to the clipboard, printing, and saving images and links.

Symantec Threat Isolation provides an Application Data Protection Profile out of the box. Activities defined in the Application Data Protection Profile are reflected in the right-click menu that appears when the end user views content, or through the end user's keyboard strokes, such as Ctrl-C for copying to the clipboard.

For more information, see section [2.5.3 "Protecting an Organization's Web Applications from Attack"](#).

4.3.8.2 Adding an Application Data Protection Profile

1. To access the Application Data Protection Profiles page, go to:
Profiles → Application Data Protection



2. Add a new Application Data Protection Profile by clicking New Application Data Protection Profile, or by cloning an existing Application Data Protection Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the table below for the new profile, and then click Create.

Parameter	Description	For More Information
Permissions		
Clipboard	<ul style="list-style-type: none">■ Copy - Enables copying/cutting webpage data to the clipboard using the keyboard or the right-click menu.<ul style="list-style-type: none">◆ Include HTML content - Allows rich text to be copied/cut from the webpage. If this checkbox is clear, rich text will be copied/cut to the clipboard as unformatted text◆ Include images - Allows images to be copied/cut from the webpage. If this checkbox is clear, no images will be copied/cut	
Print	Select to enable printing webpage data using the keyboard or the right-click menu	
Additional Resources	<p>Select the option(s) to be displayed in the context menu:</p> <ul style="list-style-type: none">■ Save image as - Opens a file dialog that enables saving a website image to the local file system■ Save link as - Opens a file dialog that enables saving the website link to the local file system■ Open developer tools remotely - Opens a file dialog that enables the remote use of developer tools	See the parameter "Context Menu" in section 4.3.3.2 "Adding an Isolation Profile"

4.3.8.3 Opening Developer Tools Remotely

Chrome Developer Tools does not work in Symantec Threat Isolation isolated sites. However, you can allow your developers to open the Developer Tools remotely when browsing in an isolated environment, as follows.



1. Do one of the following:

- ◆ To create a new Application Data Protection Profile, go to:

Profiles → Application Data Protection → New Application Data Protection Profile

- ◆ To update an existing Application Data Protection Profile, go to:

Profiles → Application Data Protection

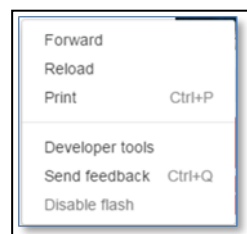
Under Actions, click the edit icon for the relevant profile.

2. Under Additional Resources, select the Open developer tools remotely checkbox.

3. Click Create to save the new profile, or Update to update the existing one.

To open the Developer Tools remotely from an isolated webpage:

1. Right-click to open the drop-down menu.





2. Choose Developer tools from the menu to open the tools.

Developer Tools opens, but the code you see is the Symantec Threat Isolation code for the isolated site. However, the tools include debug capabilities for the original HTML code of the website.

4.3.9 Defining Anti-Bot Protection Profiles

4.3.9.1 Overview

Anti-Bot Protection Profiles define settings that prevent bots inside an organization's network from reaching the Internet using the HTTP protocol.

When a new browser (or tab, depending on the configuration) is opened, an anti-bot captive page is displayed. Only real (human) end users should get past this page; bots should not.

Symantec Threat Isolation allows your organization to upload an HTML page of its own to be displayed as the captive page. In addition, customizable sample HTML pages are provided.

4.3.9.2 Adding an Anti-Bot Protection Profile

1. To access the Anti-Bot Protection Profiles page, go to:

Profiles → Anti-Bot Protection

2. Add a new Anti-Bot Protection Profile by clicking New Anti-Bot Protection Profile, or by cloning an existing Anti-Bot Protection Profile (for more information, see section [4.3.2 "Cloning Objects"](#)).
3. Configure the parameters described in the table below for the new profile, and then click Create.

Parameter	Description	For More Information
Protection Settings		
Anti-Bot Page	<p>The display mode:</p> <ul style="list-style-type: none">■ Basic Protection - Select to display Symantec Threat Isolation's standard anti-bot captive page, for basic protection■ Custom - Select to use a custom HTML page of your choice that will be displayed as the anti-bot captive page. Use the Browse button to upload the relevant HTML file	See section 4.3.9.3 "Customizing the Anti-Bot Captive Page"



Parameter	Description	For More Information
Response Timeout (Seconds)	The timeout period for the end user's response, in seconds	
Protection Scope	When the captive page will be displayed: <ul style="list-style-type: none">■ Browser-based protection - Whenever a new browser is opened■ Tab-based protection - Whenever a new tab is opened	

4.3.9.3 Customizing the Anti-Bot Captive Page

Your organization can choose to display the standard anti-bot captive page that Symantec Threat Isolation provides for basic protection, or use a customized page.

Preparing a customized anti-bot captive page

A customized anti-bot captive page can be any HTML page of your choice, as long as it is compatible with the Symantec Threat Isolation Anti-Bot interface. For this purpose, the page can make the following API calls as needed:

API	Description	Comment
<code>setTimeout</code> (<code>window.fgAntibotTimeout</code> , <code>{{anti_bot_timeout}}</code>);	The timeout elapsed with no end-user response	The <code>{{anti_bot_timeout}}</code> must be left as is. The Threat Isolation Engine (TIE) injects the timeout value from the Anti-Bot policy during runtime
<code>window.fgAntibotVerify</code> (<code>{{anti_bot_token}}</code>);	Indicates that the end user passed the anti-bot captive page	The <code>{{anti_bot_token}}</code> must be left as is. The TIE injects a unique token during runtime to prevent unauthorized usage
<code>window.fgAntibotFailed()</code> ;	Indicates that the end user failed to pass the anti-bot captive page (meaning it could be a bot)	

For your convenience, Symantec Threat Isolation also provides two customizable sample anti-bot captive pages:

- Basic sample page - This sample HTML page is identical to the standard anti-bot captive page that Symantec Threat Isolation provides for basic protection, and can be customized per your requirements. For example, you can change the default logo to that of your organization.



To download the basic sample page:

- a. Go to: Profiles → Anti-Bot Protection.
- b. Under Actions, click the edit icon for the profile.
- c. Under Basic Protection, click Download.

- Advanced sample page – This sample HTML page offers more advanced options than the basic page, for advanced protection, and can be customized per your requirements.

To download the advanced sample page:

- a. Go to: Profiles → Anti-Bot Protection.
- b. Under Actions, click the edit icon for the profile.
- c. Under Custom, click Download.

Using a customized anti-bot captive page

1. Go to: Profiles → Anti-Bot Protection.
2. Under Actions, click the edit icon for the profile.
3. Under Protection Settings, Anti-Bot Page, select Custom.
4. Use the Browse button to upload the relevant HTML file.

This can be one of the following:

- ◆ Your own anti-bot captive page (must be compatible with the Symantec Threat Isolation Anti-Bot interface).
- ◆ The basic sample page, customized per your requirements.
- ◆ The advanced sample page, customized per your requirements.
Important: When using this page, follow the inline instructions in the HTML file before uploading the file.

5. Click Update.



4.4 Defining Policy Entities

The following sections describe the Policy Entity objects. Most policy entities specify the match criteria for a policy rule. However, some exceptions define actions that Symantec Threat Isolation applies when a policy rule is matched. These exceptions are:

- Custom Page
- Rule Advanced Settings
- Policy Advanced Settings

4.4.1 Accessing Policy Entities

- To access a policy entity, go to:

Policy Entities → [Select Entity]

The following sections describe each policy entity.

4.4.2 Managing Threat Isolation in Multiple Organizations

Symantec Threat Isolation allows you to manage your policy across multiple unrelated organizations, with different domains and end users. In this scenario, activity logs are tagged with the organization to which the end user belongs. Management users are assigned to specific organizations and are allowed to view only the activity logs that relate to end users within those organizations. Private data is separated per organization to ensure that it can be viewed only by the appropriate Management user(s).

Symantec Threat Isolation tags sessions to end users who have been authenticated through identity providers (Active Directories or SAML Identity Providers). If your organization needs to be subdivided into multiple organizations, you can map one identity provider to each organization. If you want to subdivide into smaller units than identity providers, specify one or more domains for each organization.

4.4.2.1 Creating Organizations

You may need to manage the Symantec Threat Isolation policy across multiple unrelated organizations, with different domains and end users. For this purpose, you can define Organization objects for each individual organization.

1. To create an Organization object, go to:

Policy Entities → Organization → New Organization



2. Configure the parameters described in the table below for the new organization, and then click Create.

Parameter	Description	For More Information
General		
Name	Specify a name for the new organization. This name will be tagged to all Activity Logs.	
Identity		
Identity Provider	<p>Select the identity provider that references this organization's end-user directory. The drop-down list is dynamic and includes all SAML Identity Providers, all Active Directory settings, and the built-in Internal Identity Provider.</p> <ul style="list-style-type: none">■ Internal■ The SAML Identity Provider <p>NOTE: The identity provider can only be used in multiple organizations if specific domains are picked from it. Otherwise, all domains are picked. This prevents other organizations from picking domains from this identity provider.</p>	
Domains	<p>Symantec Threat Isolation takes domain names from the Identity Provider selected above. If this identity provider is shared by several organizations, specify the relevant domain name(s) for this organization.</p> <p>NOTES:</p> <ul style="list-style-type: none">■ When All Domains is selected (default), new domains will be included in this organization automatically.■ A domain name from the same identity provider can be used in only one organization.	

4.4.3 Creating Access Roles

Access roles determine when the match criteria for a rule will be applied to user name(s) or user group(s). The Access Role object contains a list of users and/or user groups.

You cannot assign a user or group to a rule directly; you must first create an Access Role object and assign users and groups to it. You can then assign the Access Role object to a rule.

1. To create an Access Role object, go to:

Policy Entities → Access Roles → New Access Roles



2. Configure the parameters described in the table below for the new access role, and then click Create.

Parameter	Description	For More Information
General		
Identity Provider	<p>Select the defined Identity Provider object from which members (see below) will be selected:</p> <ul style="list-style-type: none">■ Active Directory■ SAML Identity Provider■ Internal Identity Provider <p>NOTE: This selection does not persist. It is only used for clarity with regard to the selection of members</p>	
Members	<p>Assign end users or groups to the Access Role object.</p> <p>NOTES:</p> <ul style="list-style-type: none">■ Access roles are generic. The Access Role object is evaluated according to your selection in the Policy object, Authentication Settings Profile■ If you are adding users and/or groups from AD, or internal users, the system will autocomplete your input. If you are using SAML without an LDAP connection, you need to fill in the claims manually	<ul style="list-style-type: none">■ See section 4.5.1.1 "Creating Internal Users" for defining internal users■ See section 4.5.1.2 "Creating Internal User Groups" for defining internal user groups■ See section 4.5.2 "Defining Active Directory Settings" for Active Directory settings■ See section 4.2.2.1 "Defining Authentication Profiles" for information about defining authentication profiles

- To clear all authorization data (meaning, the authenticated username and its groups) from all active sessions, run the following command:

```
fgcli operation clear-authorization-claims
```

Note

Since this command clears all authorization data from all active sessions, it is recommended to be run after work hours.



4.4.4 Categorizing Websites

You can categorize websites to match criteria in policy rules by doing either of the following:

- Defining URL Categories – Enables you to categorize websites by their content. For example, sports, education, malware, and so on.
- Defining Risk Levels – Enables you to categorize websites by their risk level.

For website categorization, Symantec Threat Isolation uses a cloud-based infrastructure called the Symantec Global Intelligence Network (GIN). For more information, see <https://www.symantec.com/theme/global-intelligence-network>.

4.4.4.1 Defining URL Categories

1. To create a URL Category, go to:
Policy Entities → URL Categories → New URL Category
2. Specify a Name and a Description for the category.
3. Configure the parameters described in the table below for the new URL Category, and then click Create.

Parameter	Description	For More Information
Category	Add or remove a category or a parent category (for example, sports, education, malware, and so on.) that you want to allow or prohibit.	

URL Parent Categories and Categories

When you select a Parent Category, this selects all child categories under it. You can also select only some child categories under the categories. For more information, see section [4.2.7 "Defining Policy Rules"](#).

Create URL Categories

NameSecurity

DescriptionDescription

Categories

Search

+☐ Business Related (3)

+☐ Legal Liability (2)

+☐ Non-Productive (6)

-☐ Security (2) ?

-☒ Security Concerns (7) ?

>

<

☒ Dynamic DNS Host

☒ Hacking

☒ Placeholders

☒ Potentially Unwanted Softw...

☒ Remote Access

☒ Spam

Selected Categories

Search

-☐ Security (2) ?

-☐ File Transfer (3)

☐ File Storage/Sharing

☒ Peer-to-Peer (P2P)

☐ Software Downloads

-☐ Security Concerns (1) ?

☐ Compromised Sites ?

CREATE

CANCEL

4.4.4.2 Defining Risk Levels

1. To create a Risk Level, go to:
`Policy Entities → Risk Levels → New Risk Level`
2. Configure the parameters described in the table below for the new Risk Level, and then click Create.

Parameter	Description	For More Information
General		
Risk Level	<p>Drag the slider to comprise the relevant Risk Level range:</p> <ul style="list-style-type: none"> ■ Clean ■ Shady/Unproven ■ Suspicious ■ Malicious 	See section 4.2.7 "Defining Policy Rules"



4.4.5 Controlling Non-Browser Application Objects

Symantec Threat Isolation offers the granularity to protect end users when non-browser applications are used. Such applications are native applications that use the HTTP protocol even though they are not browsers; for example, Microsoft Office and Slack.

Out of the box, Symantec Threat Isolation enforces a Pass rule for a predefined list of applications. It also provides a closure Pass rule for all other applications, in order to avoid connectivity issues in your organization. It is good practice to manually change the closure Pass rule to Block, and then add the applications that your end users use and that are permitted by your organizational policy to the Pass rule, so that only these applications will pass, while all others will be blocked.

You can assign an action to an individual application or to a group of applications, as follows.

1. Go to:

Policies → My Policy → New Rule

or edit an existing rule.

2. In Match Criteria > Destination, select the relevant application or group of applications.

The table below lists the application objects that you can select, organized by group.

Notes

- Applications and groups of applications can only be used from the policy rule (see section [4.2.7 "Defining Policy Rules"](#)). Currently, no new applications or groups can be added.
- A group of applications includes only the specific applications that are listed in the table. Any other applications associated with the group's name are not included.



Group	Application	Description	Provider
Browser Services	Browser Add-on Stores	Common stores for downloading Chrome and Firefox add-ons.	N/A
	Chrome DevTools	A set of web developer tools that can help you diagnose problems quickly.	Google LLC
	Chrome Services	Common Chrome Services	Google LLC
	Firefox Services	Common Firefox Services	Mozilla Corporation
	Google Geo Location Service	Provides geocoding and reverse geocoding of locations.	Google LLC



Group	Application	Description	Provider
Collaboration Tools	Amazon Chime	Online meetings and video conferencing application.	Amazon.com, Inc.
	Bitrix24	Provides a complete suite of social collaboration, communication and management tools.	Bitrix
	BlueJeans	Interoperable cloud-based video conferencing service.	BlueJeans Network
	Google Hangouts	A communication platform that includes messaging, video chat, SMS and VoIP features.	Google LLC
	GoToMeeting	Online meeting, desktop sharing, and video conferencing software through the Internet.	LogMeIn, Inc.
	Join.Me	Meeting and online collaboration software.	LogMeIn, Inc.
	Microsoft Teams	Unified communications platform that combines persistent workplace chat, video meetings, file storage and application integration.	Microsoft Corporation
	Moxtra	Provides a private, white-labeled collaboration solution.	Moxtra, Inc.
	Riot	Enables users to communicate with their team and out of network colleagues.	Riot.im
	Skype	Telecommunications application software product that specializes in providing video chat and voice calls.	Skype Technologies
	Slack	Provides persistent chat rooms (channels) organized by topic, as well as private groups and direct messaging.	Slack
	UberConference	Live meeting app.	Dialpad
	Viber	Cross-platform instant messaging and voice over IP (VoIP) application.	Rakuten, Inc.



Group	Application	Description	Provider
	VSee	Low-bandwidth, group video chat and screen-sharing software tool.	VSee Lab, Inc.
	WebEx & Jabber	On-demand collaboration, online meeting, web conferencing and videoconferencing application.	Cisco Systems, Inc.
	Zoom	Communications software that combines video conferencing, online meetings, and mobile collaboration.	Zoom Video Communications, Inc.
File Storage and Sharing	Amazon Drive	Supports downloading/uploading files from/to cloud should they be restored.	Amazon.com, Inc.
	Backup and Sync from Google Drive	Sets certain folders to constantly sync onto their Google account's drive.	Google LLC
	Box	Enables securing, sharing and editing all files from anywhere.	Box, Inc.
	Dropbox	Secure file sharing and storage solution.	Dropbox, Inc.
	iCloud	Cloud-based system that allows users to store heterogenous music, photos, applications and documents.	Apple Inc.



Group	Application	Description	Provider
Instant Messaging	Imo Messenger	Simple and fun way to message and video chat.	imo
	Line	App for instant communications on electronic devices such as smartphones, tablet computers and personal computers.	Line Corporation, Ltd.
	Telegram	App where users can send messages and exchange photos, videos, stickers, audio and files of any type.	Telegram Messenger LLP
	WeChat	Chinese multi-purpose social media mobile application software.	Tencent Holdings Limited
	WhatsApp	Enables sending of text messages and voice calls, as well as video calls, images and other media, documents, and user location.	WhatsApp, Inc.
	Yahoo! Messenger	Advertisement-supported instant messaging client and associated protocol provided by Yahoo!	Yahoo!
Personal Use and Entertainment	Hulu	American subscription video on demand service	Hulu LLC
	iTunes	Media player, media library, Internet radio broadcaster, and mobile device management application	Apple, Inc.
	Pandora	Audio streaming platform	Pandora Media LLC
	Spotify	Digital music, podcast, and video streaming service	Spotify AB



Group	Application	Description	Provider
Productivity	Acrobat Reader	Supports viewing, printing and annotating of PDF files.	Adobe Systems Incorporated
	Evernote	App designed for note taking, organizing, tasks lists, and archiving.	Evernote Corporation
	GitHub Desktop	Open source Electron-based GitHub app.	GitHub, Inc.
	Microsoft Office	Suite of applications dedicated to producing information, such as documents, presentations and worksheets.	Microsoft Corporation
	Power BI	Interactive Data Visualization BI Tools	Microsoft Corporation
Streaming Services	Netflix	DVD rental and Internet-based video-on-demand service.	Netflix, Inc.

4.4.6 Creating Custom Pages

4.4.6.1 Creating a Custom Block Page

The application-level block page displays HTML content that the end user sees when browsing to a website that is blocked in accordance with your organization's policy.

Note

This block page must not be confused with the Symantec Threat Isolation block page, which contains Symantec Threat Isolation client-side logic for initiating WebSocket, sending user gestures, and getting isolated data in return. For more information, see section [2.2 "Returned HTML Content"](#).

When a block rule exists, the content of the application-level block page can be customized using an HTML editor. For example, dynamic values such as username can be taken from session data and injected into the page. You can define these values in the parameters described below.

1. To create a block page, go to:

Policy Entities → Custom Pages → New Custom Page → Block Page

2. Configure the parameters described in the table below for the new block page, and then click Create.



Parameter	Description	For More Information
Text and Graphic Editor		
Enables you to design the text and layout, and add graphics for your block page		
Page Variables		
Address	Address of the blocked URL	
Category	Category name of the blocked URL	
Ticket ID	<ul style="list-style-type: none">■ A unique number associated with the block action■ Used for troubleshooting where the rule associated with the Ticket ID in the activity log can provide the reason for blockage	
Username	Name of the user who got the blocked page Enables personalizing the block page by including the user's name	
Source IP	Source IP of the user who got the blocked page	
Admin E-mail	The email address of the Management user Enables end user to report problems directly to the Management user	
Risk Level	Risk level of the blocked URL	
Additional Options		
Use raw HTML editor	Check to use raw HTML content	
Add meta tags	Check to support browsers with compatibility mode	

- When defining block pages, it is possible to define exactly what information and links you want to show, such as the organization's logo, link to a specific website, and so on.
- Out of the box, Symantec Threat Isolation provides a Symantec Threat Isolation block page that can be customized to meet your organization's needs. You can customize it by adding a different logo, text, and security rules associated with it.
- It is also possible to define multiple block pages, each for a different use. For example, you can define multiple block pages, each in a different language or linked to a different security policy rule.



4.4.6.2 Creating a Custom Read-Only Page

When “Read-Only Page” is enabled in the end user’s End-User Data Protection Profile settings (see section [4.3.7 "Defining End-User Data Protection Profiles"](#) and section [4.3.7.2 "Adding an End-User Data Protection Profile"](#)), a read-only page is displayed when the user browses to a website that is deemed to be high-risk (according to the match criteria for the policy rule), and tries to type information or click on an input field or button. Thus, Read-Only mode prevents the user from submitting information to such high-risk websites. (Note that this option refers to the verdict; the match criteria for the policy rule must be specified. For more information, see section [4.4 "Defining Policy Entities"](#).)

You can customize the content of the read-only page.

1. To customize the content of the read-only page, go to:

Policy Entities → Custom Pages → New Custom Page → Read Only Page

2. Configure the parameters described in the table below, and then click Create.

Parameter	Description	For More Information
Text and Graphic Editor		
Enables you to design text and layout, and add graphics to the message that is displayed on top of the read-only page		
Page Variables		
Address	The URL of the high-risk website	
Ticket ID	<ul style="list-style-type: none">■ A unique number associated with the read-only action■ Used for troubleshooting where the rule associated with the Ticket ID in the activity log can provide the reason for the action	
Username	Name of the end user who sees the read-only page. Enables you to personalize the read-only page by including the end user’s name.	
Additional Options		
Use raw HTML editor	Check to use raw HTML content	
Use color in dialog title	Check to display a background color in the title bar of the message dialog	
Accent Color	Select the color to be displayed in the title bar of the message dialog	



4.4.7 Creating Network Objects and Object Groups

Network Objects are defined segments of a network, based on IP. Network Object Groups are collections of Network Objects. Both of these objects are used in the rule-match source/destination criteria and the PAC exclusion rules (see section [4.7.2.4 "Updating a Zone's PAC File"](#)).


When you have made your updates, close the Update Threat Isolation Engine Affinity window (see section [4.7.2.3 "Updating Threat Isolation Engine Affinity"](#)).

4.4.7.1 Defining Network Objects

1. To create a Network Object, go to:

Policy Entities → Network Objects → New Network Object → Network Object

2. Configure the parameters described in the table below for the new Network Object, and then click Create.

Parameter	Description	For More Information
General		
Type	Can be one of the following: <ul style="list-style-type: none">■ IP address■ IP range■ Subnet/mask	
Value		
Value	<ul style="list-style-type: none">■ IP addresses or other values associated with the Type■ Enter the individual value and click the +ADD button, or click the Advanced Settings button  to add multiple values	

4.4.7.2 Defining Network Object Groups

1. To create a Network Object Group, go to:

Policy Entities → Network Objects → New Network Object → Network Object Group

2. Configure the parameters described in the table below for the new Network Object Group, and then click Create.




Parameter	Description	For More Information
General Properties		
Network objects	Network objects associated with this group	See section 4.4.7.1 "Defining Network Objects"

4.4.8 Creating URL Objects and Object Groups

URL objects are defined segments of a network, based on URL. These objects are used in the rule-match Destination criteria. URL objects can be associated with URL object groups.

4.4.8.1 Creating URL Objects

- To create a URL Object, go to:
`Policy Entities → URL Objects → New URL Object → URL Object`
- Configure the parameters described in the table below for the new URL Object, and then click Create.

Parameter	Description	For More Information
General		
Type	Select one of the following: <ul style="list-style-type: none">■ Host Name■ Wildcard■ Regular Expression	
Value		
Value	<ul style="list-style-type: none">■ Host names or other values associated with the Type■ Specify the individual value and click the +ADD button, or click the Advanced Settings button  to add multiple values	

4.4.8.2 Creating URL Object Groups

- To create a URL Object Group, go to:
`Policy Entities → URL Objects → New URL Object → URL Object Group`
- Configure the parameters described in the table below for the new URL Object Group, and then click Create.



Parameter	Description	For More Information
General Properties		
URL objects	Select URL objects associated with this group	See section 4.4.8 "Creating URL Objects and Object Groups" 4.4.8 "Creating URL Objects and Object Groups"

4.4.9 Creating Request Filters

In some cases, you might want to define rule match criteria that are more granular than “Source” or “Destination”. For example, you might need to distinguish a rule by HTTP request method, the existence of a specific header name, or its value. For this purpose, you can define request filters.

4.4.9.1 Creating a Request Filter

- To access Request Filters and define a new Header Criteria Filter, go to:

Policy Entities → Request Filters → New Request Filter

The table below summarizes the parameters you can configure for each HTTP headers filter.

Parameter	Description	For More Information
General		
Method	HTTP methods used. Can be one of the following: <ul style="list-style-type: none">■ GET■ POST■ PUT■ DELETE■ CONNECT■ HEAD■ TRACE■ OPTIONS■ PATCH Leaving this field empty signifies any method	
Headers Criteria		
Headers Criteria	All criteria in the HTTP headers must be matched. Leaving this field empty signifies any header.	



Parameter	Description	For More Information
Add Header Criteria	Adds new header criteria to the header criteria area. Leaving this field empty signifies any header.	See section 4.4.9.2 "Creating Header Criteria"
Data Criteria		
Data Criteria	Data criteria in the body or the query parameters to be matched.	
Add	Add data criteria to the text box.	See section 4.4.9.3 "Creating Data Criteria"
Notify End User	When a top-level navigation resource and/or a subresource is blocked because data criteria were matched, the end user is notified via a Data Protection pop-up message. Select one of the following options: <ul style="list-style-type: none">■ Notify only for top-level navigation■ Notify for both top-level navigation and subresources (default)	See section 8.5 "Data Protection"

4.4.9.2 Creating Header Criteria

- To access Request Filters and define a new Header Criteria Filter, go to:
Policy Entities → Request Filters → New Request Filter → Add Header Criteria

The table below summarizes the parameters you can configure for each header criterion.

Parameter	Description	For More Information
Header Name	Name of HTTP header to be matched	
Match header if	<ul style="list-style-type: none">■ Header value matches: Regex match pattern for the header's value■ Header name does not exist	



- The Header Criteria area enables you to do the following:
 - ◆ Add, edit, or delete HTTP header criteria.
 - ◆ Search for existing criteria using the search bar. When you find the criterion you are searching for, it is added to the Header Criteria area.

4.4.9.3 Creating Data Criteria

You can add data criteria as regular expressions (regex) to search for in the body of a network request and query parameters.

1. To access Request Filters and define a new Data Criteria filter, go to:
`Policy Entities → Request Filters → New Request Filter`
2. In the Data Criteria section, do one of the following:
 - ◆ Specify a criterion as a regular expression (regex), and then click Add to add it to the Data Criteria text box.
 - ◆ Search for an existing criterion using the search bar. When the criterion is found, it is added to the Data Criteria text box.

4.4.10 Creating Rule Advanced Settings

Standard rule settings might not always provide sufficient granularity. For advanced scenarios, Symantec offers a vast number of settings that provide rich additional granularity.

1. To create a Rule Advanced Setting, go to:
`Policy Entities → Rule Advanced Settings → New Rule Advanced Setting`
2. Configure the parameters described in the table below for the new Rule Advanced Setting, and then click Create.

Parameter	Description	For More Information
Website Subresources Policy		



Parameter	Description	For More Information
Fallback Action for Non-isolable Subresources	<p>(This setting is relevant when the general website is bypassed while its subresource is matched with an Isolate rule.)</p> <p>Select a fallback action to be performed when a subresource that cannot be isolated* is matched with an Isolate rule:</p> <ul style="list-style-type: none">■ Block■ Inspect - When this option is selected, the download policy will be applied by the Inspect Advanced Settings in the corresponding Download Profile■ Pass <p>*Only HTML type resources, such as iframes, and PDFs can be isolated</p>	See section 4.3.4.4 "Adding a Download Profile" the Inspect Advanced Settings parameter
Isolation Policy for Files	<p>Select the rule action to apply to files that reside in a bypassed website. HTML and PDF files are always isolated.</p> <ul style="list-style-type: none">■ Isolate HTML and PDF only. With this option, files that are not isolated are subject to the Fallback Action for Non-isolable Subresources.■ Isolate all supported file types.	For a list of supported file types, see 4.3.4 "Defining Download Profiles" , View action.
Isolation Policy for iframes	<p>Select the rule action to be applied to iframes that reside in a bypassed website:</p> <ul style="list-style-type: none">■ Inspect - When this option is selected, the download policy will be applied by the Inspect Advanced Settings in the corresponding Download Profiles■ Isolate - When this option is selected, only the iframe will be isolated. <p>NOTE: Some web pages communicate with the iframes residing in them. By default, communication between an isolated iframe and the non-isolated main page is enabled to ensure that the iframe does not break.</p> <ul style="list-style-type: none">■ Pass	See section 4.3.4.4 "Adding a Download Profile" Inspect Advanced Settings parameter
Settings		



Parameter	Description	For More Information
Isolation Suspension	<ul style="list-style-type: none">■ Select to allow the end user to open the same webpage in Pass mode for a configurable period of time<ul style="list-style-type: none">◆ Select to require the end user to provide justification for the suspension◆ Suspension time period is configurable◆ Select to inspect content when isolation is suspended. When this option is selected, the Inspect action and not the Pass action will be enforced when the end user suspends isolation	See section 4.4.10.1 "Enabling the End User to Temporarily Suspend Isolation "
Idle Mode	<ul style="list-style-type: none">■ Select to stop rendering when no mouse or keyboard input is detected (favors performance)■ Switch to idle mode after configurable number of seconds	See section 4.4.10.2 "Idle Mode Setting"
Internal Settings	Edit button that enables editing of rule's advanced internal settings NOTE: Contact Symantec Threat Isolation technical support for assistance with these settings	

4.4.10.1 Enabling the End User to Temporarily Suspend Isolation

When necessary, you can enable individual end users to temporarily suspend isolation of a specific webpage. Suspending isolation will affect only that specific website for the configured amount of time. You can allow trusted, sophisticated end users, who are aware of the risks of Internet browsing, to do this when they have a need to bypass the isolation sandbox.

1. Define a new rule for accessing the specific webpage and permitted users. See sections [4.2.7 "Defining Policy Rules"](#) (defining rules) and [4.4.10 "Creating Rule Advanced Settings"](#) (defining users), respectively.
2. In the Advanced Settings for this rule, select Allow end user to suspend isolation.

When this setting is selected, the end user can open the same webpage in Pass or Inspect mode (depending on whether you selected Perform content inspection when isolation is suspended) for the period of time specified by the Management user.



Create Rule Advanced Settings

General

Name ✓

Description

Settings

Isolation Suspension

☐ Allow end-user to suspend isolation

☐ Require justification

Suspension applies for 60 minutes

☐ Perform content inspection when isolation is suspended

Idle Mode ✓ Stop rendering when no mouse or keyboard input is detected (favors performance)

Switch to idle mode after 60 seconds ✓

Internal Settings [EDIT...](#)

[CREATE](#) [CANCEL](#)

3. To require a justification from the end user who wants isolation to be suspended, select **Require Justification**.

When this setting is checked, a pop-up menu opens when the end user right-clicks the isolated webpage. When **Suspend Isolation** is chosen from the menu, the user is prompted for a justification.

4. Set the interval length, in minutes, during which you allow the end user to suspend isolation.
5. Select **Perform content inspection when isolation is suspended**, to make Symantec Threat Isolation enforce the **Inspect** action rather than the **Pass** action when the end user suspends isolation.
6. Click **Create**.

4.4.10.2 Idle Mode Setting

When the **Idle Mode** setting is selected, the continual rendering of an isolated website stops when no mouse action occurs, thus providing savings in performance. When **Idle Mode** is deactivated, rendering continues for every change that takes place in the Internet site. Note that audio is not affected by **Idle Mode** settings.



4.4.11 Creating Policy Advanced Settings

Standard policy settings might not always provide sufficient granularity. For advanced scenarios, Symantec offers a vast number of settings that provide rich additional granularity.

1. To create a Policy Advanced Setting object, go to:
`Policy Entities → Policy Advanced Settings → New Policy Advanced Setting`
2. Configure the parameters described in the table below for the new Policy Advanced Setting object, and then click Create.

Parameter	Description	For More Information
Session Activity Settings	<ul style="list-style-type: none">■ Select to enable terminating a session when no user activity is detected ("idle") for the specified number of seconds. This setting enhances performance. Default: Disabled■ Specify the number of seconds a session must be idle before it is terminated. Default: After 3600 seconds■ Possible exceptions to the setting (when Session Activity Settings is enabled, all of these are enabled by default):<ul style="list-style-type: none">◆ Not during file transfer◆ Not during media streaming◆ Not when the tab is in the foreground	
Advanced		
Internal Settings	<p>Edit button that enables editing the policy's advanced internal settings</p> <p>NOTE: Contact Symantec Threat Isolation technical support for assistance with these settings</p>	

4.4.12 Creating Geolocation Objects

The Geolocation object allows you to specify one or more destination countries as match criteria.

1. To create a Geolocation object, go to:
`Policy Entities → Geolocation objects → New Geolocation object`
2. Configure the parameters described in the table below for the new geolocation, and then click Create.



Parameter	Description	For More Information
Countries	Destination countries to include in the object	
Unknown Location	IP addresses that are not associated with a geographic region and are therefore unknown	

4.5 Defining Internal Users

This section explains how to define internal users and user groups that browse the isolated websites.

4.5.1 Creating Internal Users and User Groups

When no external user directory exists, such as Active Directory or SAML server, you can use the Symantec Threat Isolation User Directory. This User Directory is pushed to all Threat Isolation Gateways, thus avoiding the need for an additional authentication server. It is commonly used in demos, where no organizational user directory exists.

4.5.1.1 Creating Internal Users

1. To create an internal User object, go to:
User Management → Internal Users → New User
2. Configure the parameters described in the table below for the new internal user, and then click Create.

Parameter	Description	For More Information
Name	Unique username that identifies the internal user	<ul style="list-style-type: none">■ See section 4.2.2.1 "Defining Authentication Profiles" for information about defining authentication profiles■ See section 4.4.3 "Creating Access Roles" for information about access roles
Password	Unique password for the internal user	See section 3.11.3.1 "Password Policy" for a detailed explanation of the password policy.
Email	Internal user's email address	
Groups	Internal user group(s) to which this internal user is assigned (or none)	See section 4.5.1.2 "Creating Internal User Groups"



4.5.1.2 Creating Internal User Groups

1. To create an internal user Group object, go to:
User Management → Internal Groups → New Group
2. Configure the parameters described in the table below for the new internal user group, and then click Create.

Parameter	Description	For More Information
Group name	Unique name for this internal user group	<ul style="list-style-type: none">■ See section 4.2.2.1 "Defining Authentication Profiles" for information about authentication profiles■ See section 4.4.3 "Creating Access Roles" for information about access roles

Note

Currently, you cannot populate an internal user group from the Group object. You can only assign internal users to a group from the User object. For more information, see section [4.5.1.1 "Creating Internal Users"](#)

4.5.2 Defining Active Directory Settings

If your organization uses the Active Directory (AD) database to maintain its employees, you need to define the AD settings used for Symantec Threat Isolation access to the AD database.

1. To create AD settings, go to:
User Management → Active Directory Settings → New Active Directory Settings
2. Configure the parameters described in the table below for the new Active Directory settings, and then click Create.

Parameter	Description	For More Information
Active Directory Settings		
Domain name	Specify the AD domain name	
Domain controller	Specify the IP address or resolvable host name of the AD domain controller	
Global Catalog (optional)	Specify the Global Catalog host. A Global Catalog is a data storage source containing partial representations of objects found in a multidomain Active Directory Domain Services (AD DS) forest	



Parameter	Description	For More Information
Directory access service account		
Username	Specify an existing ADy username	See Note 1, below
Password	Specify the password for the above username	See Note 1, below
Use SSL for Active Directory connections	Select to use the LDAPS protocol (secured) If this checkbox is clear, the LDAP protocol will be used	

Notes

- The username and password are used by the Threat Isolation Gateway during the authorization phase, which involves checking the match criteria of the access roles. They are also used by the Symantec Threat Isolation Management component when filling in users and user groups from AD in the Access Role object UI pickers.
- You can only define AD groups through Active Directory. From the Symantec Threat Isolation Management UI, you can select AD groups from the Access Profile pages.

4.5.3 Creating Keytab Settings

When an Active Directory authentication profile is used, you must supply a keytab, which is required for the Kerberos protocol. A keytab must contain at least one Principal name, but additional Principal names might be added. For more information, see section [4.5.3.1 "Keytab Requirements"](#).

1. To create a Keytab Settings object, go to:
`User Management → Keytab Settings → New Keytab Settings`
2. Configure the parameters described in the table below for the new Keytab Settings object, and then click Create.

Parameter	Description	For More Information
General		



Parameter	Description	For More Information
Public DNS Name	<p>The Keytab Settings object will be applied to all Threat Isolation Gateways, using one of the selected Public DNS names</p> <p>Notes:</p> <ul style="list-style-type: none">■ A Keytab Settings object can be applied to more than one Gateway■ Assigning Public DNS names to the Keytab Settings object enables you to assign multiple keytabs to the same Gateway	
Instructions		
When the Gateways' Public DNS names have been specified, detailed instructions for creating the keytab file are displayed		
Keytab File		
Keytab	Browse to the keytab file location and upload the file	
Diagnostics		
When the keytab file has been uploaded, diagnostics are displayed, confirming the association between the keytab Principal and the related Gateways		

4.5.3.1 Keytab Requirements

The Kerberos protocol has the following specific requirements to ensure authentication:

- Principal keytab name – The full Principal name must be formatted as:
`HTTP/<machine.name.here> @ <DOMAIN.NAME>`
- The machine name must be a registered name in the DNS.
- UDP port 88 is used by default and must be opened from the Threat Isolation Gateway to Active Directory (AD). See section [3.6.1.4 "Defining Firewall Rules"](#) for the Explicit Proxy settings, and [3.6.5.1 "Defining Firewall Rules"](#) for Web Application Isolation Gateways.
- The machine name must be defined in the Threat Isolation Gateway as either the hostname or the Public DNS name. See section [4.7.7 "Defining a Threat Isolation Gateway"](#) for Gateway setup.



- The machine time and the Domain Controller time must be synchronized. You must enable the NTP server on the Gateway, see section [4.7.7 "Defining a Threat Isolation Gateway"](#), or synchronize the two machines manually.
- The domain name must be in upper case letters and must match the actual AD domain name of the network.
- If multiple Gateways share the same DNS, then they can share the same Principal.
- When viewing the diagnostics in the Keytab page, clicking the > symbol to the left of each row offers additional information.

4.5.4 Defining SAML Trust

Security Assertion Markup Language (SAML) is an XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between a service provider (SP) and a SAML identity provider (IdP). SAML provides single sign-on authentication for cloud applications via the authentication server.

In the Symantec Threat Isolation Platform:

- The service provider is the Threat Isolation Gateway
- The identity provider can be any SAML-capable identity provider, such as Microsoft Active Directory Federation Services (AD FS) or Okta

When the browsing policy requires SAML authentication, the Gateway redirects the request to the specified identity provider. The identity provider verifies the user credentials and returns an assertion to the browser. The assertion is then sent to the Gateway as the service provider for authentication. For information about the authentication flow, see section [4.2.2.2 "Authentication Mode": "Server Authentication Mode"](#).

When multiple Gateways share the same Public DNS name, a single SAML Trust object can be reused with several different Gateways. However, some topologies require more than one SAML Trusts object, for example in the case of a network with multiple endpoints where the Gateways do not share the same Public DNS name. For such cases, Symantec Threat Isolation allows you to define multiple SAML Trust objects, each of which is assigned to its own Gateway.

**Note**

SAML Trust objects are only applicable to Gateways that are responsible for authentication logic; that is, when the Threat Isolation Proxy component is enabled, or when the Threat Isolation Engine (TIE) is enabled with Web Application Isolation. For more information, see sections [4.7.7.2 "Enabling Web Application Isolation Gateway Mode with a Load Balancer"](#) and [4.7.8.1 "Enabling Web Application Isolation Gateway Mode - No Load Balancer"](#).

Creating a SAML Trust object

1. To create a SAML Trust object, go to:

User Management → SAML Trust → New SAML Trust

The table below summarizes parameters you can configure for the SAML Trust object.

Parameter	Description	Default
General		
Identity Provider Type	Select the identity provider to which this SAML Trust belongs	Your SAML Identity Provider
IdP Type	Select the type of the identity provider: <ul style="list-style-type: none">■ Microsoft AD FS - Microsoft Active Directory Federation Services■ Generic SAML - Another SAML-capable identity provider, such as Okta NOTE: The selected identity provider type cannot be changed afterwards.	
Configuration Mode	Select Fill in IdP details later, if you want to configure identity provider information later on (relevant if this application has not yet been configured in the identity provider). Otherwise, leave the checkbox clear	

2. Perform the relevant procedure:
 - ◆ For Microsoft AD FS, go to section [4.5.4.1 "Defining SAML Trust for Microsoft AD FS"](#)
 - ◆ For other SAML-capable identity providers, such as Okta, go to section [4.5.4.2 "Defining SAML Trust for Generic SAML Identity Providers"](#)



4.5.4.1 Defining SAML Trust for Microsoft AD FS

1. In the Symantec Threat Isolation SAML Trust, leave the Fill in identity provider details later checkbox clear.
2. Specify the service provider details as described in the following table.

Note

By default, only the Host Name field is displayed. Once it is specified, the remaining parameters will be set automatically.

Parameter	Description	For More Information
Service Provider Details		
Host Name	<ul style="list-style-type: none">■ The hostname of the service provider that the client is referred back to by the identity provider after successfully authenticating, with the user information■ If load balancing is used, the assertion consumer service hostname would be the hostname of the load balancer of the Proxies/Gateways acting as reverse proxies■ The hostname is used for the role of assertion consumer service, as defined in the SAML standard	
Metadata (hidden by default)		
Issuer	A unique identifier provided by the identity provider. This value is part of the service provider metadata. It is based on the Host Name value, but you can change it to a different value if necessary	See section 4.5.4.3 "Identity Provider (IdP) Requirements"
Callback URL	The URL that the browser is redirected to by the identity provider after successful authentication	
Logout URL	The identity provider redirects the user to this URL when they log out of the session. If logout is initiated from Threat Isolation, the identity provider is also notified to delete any cookies and that the session has completed by calling the identity provider's logout URL	
Certificate	A certificate file used to secure communication with the service provider. Browse to upload the .pem file	



3. Specify the identity provider details. Do one of the following:

- ◆ Click Import to populate the fields automatically. Select the relevant option:
 - From URL... - Change the suggested URL to your AD FS metadata URL
 - From file on computer - Provide a metadata file
- ◆ Specify the information manually, as described in the following table.

Parameter	Description
Identity Provider Details	
Entrypoint URL	The FQDN web address of the identity provider. This address is provided by the identity provider
Logout URL	Redirects the user to the specified URL when they log out of the session
Signing Certificate	Certificate file used for trusting assertions made by the identity provider. Browse to upload the .pem file

The Claims fields are displayed with their recommended values automatically:

Parameter	Description	Default
Claims		
Username Attribute	The user attribute in the assertion that the identity provider returns on successful authentication	nameID Make sure to create a Claim Rule in the AD FS Configuration to map between “SAM Account Name” to “Name ID”
Username Identifier Format	The user value format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Groups Attribute	The group attribute in the assertion that the identity provider returns on successful authentication	http://schemas.xmlsoap.org/claims/Group Make sure to create a Claim Rule in AD FS Configuration to map between “Token-Groups - Unqualified Names” and “Group”

4. Specify the information described in the table below.

Parameter	Description	Default
Advanced		



Parameter	Description	Default
User Domain	Symantec Threat Isolation extracts the user domain name from the Username value or from an attribute, and uses it to find the organization to which the domain belongs. Select the relevant option: <ul style="list-style-type: none">■ Extract from Username value (default)■ Obtain from claims attribute■ Domain Attribute (optional)	
Advanced Settings	Click Edit to display advanced settings	

5. Click Create; the SAML Trust object is created.

6. Provide the service provider details to Microsoft AD FS:

Under “Does the identity provider support importing a metadata file?”, select the relevant option:

- ◆ Yes – Select this option and then click Export. A metadata XML file is downloaded, containing the required information. Import this file into Microsoft AD FS
- ◆ No – Select this option to specify the service provider information manually

You must enable the SAML authentication for your defined profile. For more information, see section [4.2.2.1 "Defining Authentication Profiles"](#).

There must be connectivity between the client and the identity provider. For more information, see section [4.5.4.4 "Connectivity between Client and Identity Provider \(IdP\)"](#).

Note

SAML identities can be retrieved from the LDAP server and used for autocompleting information in the Access Roles page. For more information, see section [4.5.5 "Defining SAML Identity Providers"](#).

4.5.4.2 Defining SAML Trust for Generic SAML Identity Providers

The procedures explained below enable you to define SAML Trust for non-Microsoft AD FS, generic SAML identity providers, such as Okta.

To allow the service provider and the identity provider to communicate with each other, you must define the following identity provider information in the SAML Trust object: Entrypoint URL, Logout URL and Signing Certificate. Some SAML systems provide this information without preconditions, while others require you to supply initial service provider details first, before they provide their own



information. First, find out to which of these types your identity provider belongs. Then proceed to the appropriate procedure below:

- SAML systems that **do not** require service provider details first, or
- SAML systems that require service provider details first

SAML systems that do not require service provider details first

Prerequisite: Make sure your identity provider will export the required information (Entrypoint URL, Logout URL and Signing Certificate) *without* preconditions.

1. In the Symantec Threat Isolation SAML Trust dialog, leave the Fill in IdP details later checkbox clear.
2. Specify the service provider details as described in the table below.

Note

By default, only the Host Name field is displayed. Once it is specified, the remaining parameters will be set automatically.

Parameter	Description	For More Information
Service Provider Details		
Host Name	<ul style="list-style-type: none">■ The hostname of the service provider that the client is referred back to by the identity provider after successfully authenticating, with the user information■ If load balancing is used, the assertion consumer service hostname would be the hostname of the load balancer of the Proxies/Gateways acting as reverse proxies■ The hostname is used for the role of assertion consumer service, as defined in the SAML standard	
Metadata (hidden by default)		



Parameter	Description	For More Information
Issuer	A unique identifier provided by the identity provider. This value is part of the service provider metadata. It is based on the Host Name value, but you can change it to a different value if necessary	See section 4.5.4.3 "Identity Provider (IdP) Requirements"
Callback URL	The URL that the browser is redirected to by the identity provider after successful authentication	
Logout URL	The identity provider redirects end users to this URL when they log out of the session. If logout is initiated from Symantec Threat Isolation, the identity provider is also notified to delete any cookies and that the session has completed by calling the identity provider's logout URL	
Certificate	A certificate file used to secure communication with the service provider. Browse to upload the .pem file	

3. Specify the required identity provider information. Do one of the following:

- ◆ Click Import to populate the fields automatically. Select the relevant option:
 - From URL... - Change the suggested URL to your AD FS metadata URL
 - From file on computer - Provide a metadata file
- ◆ Specify the information manually, as described in the table below.

Parameter	Description
Identity Provider Details	
Endpoint URL	The FQDN web address of the identity provider
Logout URL	Redirects the user to the specified URL when they log out of the session
Signing Certificate	Certificate file used for trusting assertions made by the identity provider. Browse to upload the .pem file

Specify the Claims values, as described in the table below.

Parameter	Description	Default
Claims		



Parameter	Description	Default
Username Attribute	The user attribute in the token that the SAML identity provider returns on successful authentication	
Username Identifier Format	The user value format	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Groups Attribute	<p>The group attribute in the token that the SAML identity provider returns on successful authentication</p> <p>NOTE: When working with Azure Federation Services (FS), policies must be based on a specific user or on “all authenticated users”. This is because Azure FS cannot send group information as an attribute</p>	

4. Specify the information described in the table below.

Parameter	Description	Default
Advanced		
User Domain	<p>Symantec Threat Isolation extracts the user domain name from the Username value or from an attribute, and uses it to find the organization to which the domain belongs. Select the relevant option:</p> <ul style="list-style-type: none">■ Extract from Username value (default)■ Obtain from claims attribute	
Advanced Settings	Click Edit to display advanced settings	

5. Click Create; the SAML Trusts object is created.



6. Provide the service provider details to the identity provider:

Under “Does the identity provider support importing a metadata file?”, select the relevant option:

- ◆ Yes – Select this option and then click Export. A metadata XML file is downloaded, containing the required information. Import this file into the identity provider
- ◆ No – Select this option to specify the service provider information manually

You must enable the SAML authentication for your defined profile. For more information, see section [4.2.2.1 "Defining Authentication Profiles"](#).

There must be connectivity between the client and the identity provider. For more information, see section [4.5.4.4 "Connectivity between Client and Identity Provider \(IdP\)"](#).

Note

SAML identities can be retrieved from the LDAP server and used for autocompleting information in the Access Roles page. For more information, see section [4.5.5 "Defining SAML Identity Providers"](#).

SAML systems that require service provider details first

1. Select the Fill in IdP details later checkbox to create the SAML Trust object with only the service provider parameters defined. By selecting this checkbox, you postpone specifying the required identity provider information until later.
2. Specify the service provider details, as described above.
3. Click Create; the SAML Trust object is created.

4. Provide the service provider details to the identity provider:

Under “Does the identity provider support importing a metadata file?”, select the relevant option:

- ◆ Yes – Select this option and then click Export. A metadata XML file is downloaded, containing the required information. Import this file into the identity provider
- ◆ No – Select this option to specify the identity provider information manually

**Note**

By checking the Fill in identity provider details later checkbox, you have chosen to create this SAML Trust object with only the service provider parameters defined, and to postpone providing the required identity provider information until later. Until you have completed creating the SAML Trusts object by adding the identity provider information, the object will not appear in the list of SAML Trusts objects in the Gateway dialog, and a warning will be displayed in the SAML Trust screen.

To complete SAML Trusts configuration:

When you have provided the service provider details to the identity provider and it has provided the required identity provider information in return, do the following:

1. Open the SAML Trust object and specify the SAML identity provider information in Update mode. Do one of the following:
 - ◆ Click Import to populate the fields automatically. Select the relevant option:
 - From URL... - Change the suggested URL to your AD FS metadata URL
 - From file on computer - Provide a metadata file
 - ◆ Specify the information manually (for a description of the parameters, see the relevant table above under Identity Provider Details).

The Claims fields are displayed with their recommended values automatically.

2. Click Update.

You must enable the SAML authentication for your defined profile. For more information, see section [4.2.2.1 "Defining Authentication Profiles"](#).

There must be connectivity between the client and the identity provider. For more information, see section [4.5.4.4 "Connectivity between Client and Identity Provider \(IdP\)"](#).

Note

SAML identities can be retrieved from the LDAP server and used for autocompleting information in the Access Roles page. For more information, see section [4.5.5 "Defining SAML Identity Providers"](#).



4.5.4.3 Identity Provider (IdP) Requirements

The identity provider might require a metadata file containing the required service provider information. You can download this metadata file in the following ways:

- At the final step of creating the SAML Settings object:
Under “Does the identity provider support importing a metadata file?”, select Yes and then click Export. The metadata XML file is downloaded. Import this file into the identity provider.
- After the SAML Settings object has been created:
Open the SAML Settings in Update mode, and download the metadata file from the Export button in the Service Provider Details area.

Notes

- If any settings are changed from the Service Provider Details screen, the metadata file must be regenerated and uploaded to the identity provider. This recreates the trust between the two entities.
- If the identity provider requires user and group fields that are different than email and existing groups, contact Symantec Threat Isolation technical support.

4.5.4.4 Connectivity between Client and Identity Provider (IdP)

When SAML authentication is used, the client is redirected to the identity provider's URL to authenticate. To ensure connectivity between the client and the identity provider, do the following (choose the relevant option):

- If the Threat Isolation Proxy has access to the identity provider:
In Symantec Threat Isolation Management, create a rule:
 - ◆ Action: Bypass
 - ◆ User: Any (empty)
 - ◆ Destination: the identity provider

This rule must be ordered first.



- If the Threat Isolation Proxy does not have access to the identity provider (meaning that the client must have direct access to it):
 - ◆ In case a PAC file is configured in the endpoint browser (for more information, see section [3.6.1.2 "Configuring the PAC File in a Single Endpoint Browser"](#)):

The PAC file includes two exclusion objects out-of-box.

 - If the identity provider is included in these exclusion objects, no action is required.
 - Otherwise, create a proxy exclusion object and add it to the PAC file exclusion objects. For more information, see section [4.7.2.4 "Updating a Zone's PAC File"](#).
 - ◆ In case no PAC file is configured in the endpoint browser:
 - If your identity provider is defined as a local address, go to your Internet Options > Connections tab > LAN settings. In the Proxy server section, make sure Bypass proxy server for local addresses is checked.
 - Otherwise, click Advanced and add it to the Exceptions.

4.5.5 Defining SAML Identity Providers

The SAML Identity Provider object allows authentication through SAML. This object represents a scope for SAML identities that can be selected when you define Access Roles. Optionally, SAML identities can be retrieved from an LDAP server to be used for autocompleting information in the Access Roles page. Every SAML Trust object in the system must be assigned to a SAML Identity Provider.

1. To create a SAML Identity Provider object, go to:

User Management → SAML Identity Providers → New SAML Identity Provider

2. Configure the parameters described in the table below for the new SAML Identity Provider.

Parameter	Description	For More Information
Advanced		
Use LDAP to autocomplete Access Role member	<ul style="list-style-type: none">■ Enables usernames to be autocompleted when they are added to an Access Role. This is done using an LDAP query against the directory■ Click LDAP Settings to proceed to LDAP configuration	See section 4.5.5.1 "LDAP Access Role"

3. Configure the LDAP settings described in the table below.



Parameter	Description	For More Information
Domain Name	The name of the domain served by the domain controller	
Domain Controller	The IP address or resolvable host name of the domain controller that can accept LDAP queries	
Global Catalog (Optional)	The IP address or resolvable host name of the Global Catalog server that can accept LDAP queries for all domains contained in the Active Directory forest	
Username	The username	
Password	The password	
Security	Select to use TLS to secure communication	

4. Click Create.

4.5.5.1 LDAP Access Role

The Lightweight Directory Access Protocol (LDAP) is an industry standard for accessing and maintaining distributed directory information services over the Internet. LDAP is used in conjunction with Security Assertion Markup Language (SAML) to facilitate a single sign-on environment.

Utilizing LDAP maximizes accuracy by populating the usernames and groups as a drop-down menu selection while creating the Access Role. This efficiency leads to a granularity of detail that is easy to maintain for the organization.

If there is no access to LDAP, you can enter the usernames and group names manually as they appear in the SAML claims to the Access Roles.

For information about how to define the LDAP Access Role, see section [4.4.3 "Creating Access Roles"](#).

When SAML authentication is selected, SAML identities can be retrieved from the LDAP server and used for autocompleting information in the Access Roles page. For more information, see section [4.5.5 "Defining SAML Identity Providers"](#).



4.6 Defining Management Users

If multiple users will be logging in to the Management console, you must create a Management User object for each of these users. If your organization uses a RADIUS server or a SAML Identity Provider, you can create RADIUS Identity Provider or SAML Identity Provider objects instead (see section [4.6.2 "Identity Providers"](#)). In either case, the system will use the “super admin” created in the First Time Wizard when the Management Gateway was defined. (By default, this user is named “admin”. For added security it is recommended to specify a different username in the First Time Wizard or afterwards. For more information, see section [3.5.7 "Defining the Management Gateway"](#).)

4.6.1 Creating Management Users

Create a Management User object for each user that will login to the Management console, as follows.

Note

A Management user must be assigned to at least one Management role to be able to login to the system. For more information, see section [4.6.3 "Management Roles"](#).

1. To create a Management User object, go to:
Management → Management Users → New Management User
2. Configure the parameters described in the table below for the new Management user, and then click Create.

Parameter	Description	For More Information
General		
Username	Unique user name for this Management user	
Email	Email address of the Management user	
Password		
Password	Password for the username above	See section 3.11.3.1 "Password Policy" for a detailed explanation of the password policy
Authorization		
Roles	Management role(s) to which this Management user is assigned	See section 4.6.3 "Management Roles"



Parameter	Description	For More Information
Organizations	<p>Select the organization(s) to which this Management user is assigned:</p> <ul style="list-style-type: none">■ All organizations - Select this option only if this Management user needs viewing access to Activity Logs in all organizations■ Specific organization(s) - Select the relevant organization(s) from the drop-down list <p>NOTE: This Management user will be allowed to view only those Activity Logs that relate to end users belonging to the selected organizations</p>	<p>See section 4.4.2 "Managing Threat Isolation in Multiple Organizations"</p>

4.6.1.1 Configuring a Terms of Use Page for Management Users

When logging into the Management console, you can display a Terms of Use page to the user.

To add a Terms of Use page,

1. Go to:
System Configuration → Advanced Configuration
2. Set `shouldShowTermsOfUse` to true.
3. Under `termsOfUseHeader`, enter the header.
4. Under `termsOfUseContent`, delete the default filler text and enter content for the body of the message. This text can be html code and include colors and different fonts.
5. Under `termsOfUseUserAgreement`, change the confirmation text if necessary.



4.6.2 Identity Providers

For authentication of Management users, Symantec Threat Isolation provides the following options:

- Internal authentication – Provided out of the box
- RADIUS provider – If your organization has a RADIUS server, you can create RADIUS Identity Provider objects and delegate authentication to your organization's identity provider
- SAML provider - You can create SAML Identity Provider objects and perform the authentication on a SAML identity provider. For information about SAML Identity Providers, see section [Defining SAML Identity Providers](#).

4.6.2.1 Creating RADIUS Identity Providers

RADIUS attributes are used as criterion keys and values in Management roles. For more information, see section [4.6.3.1 "Assigning Members to Management Roles"](#).

1. To create a RADIUS Identity Provider object, go to:
Management → Identity Providers → New Identity Provider
2. From the New Identity Provider drop-down, select RADIUS Provider.
3. Configure the parameters described in the table below for the new RADIUS Identity Provider object, and then click Create.

Parameter	Description	For More Information
General		
Active	Defines whether or not this provider is available at logon time	
Connection		
Hosts	Comma-separated ordered list of hosts. Each host contains the URL address of the Identity Provider and the port through which this server communicates. The port is configurable; it can be specified after the colon in the comma-separated ordered list of hosts. For example, server1.corp:1812, server2.corp:1645, and so on	
Secret	Shared secret used in RADIUS messages	



4.6.2.2 Creating SAML Identity Providers

SAML attributes are used as criterion keys and values in Management roles. For more information, see section [See "Assigning Members to Management Roles" on page 218.](#)

1. To create a SAML Identity Provider object, go to:
Management → Identity Providers → New Identity Provider
2. From the New Identity Provider drop-down, select SAML Identity Provider.
3. Configure the parameters described in the tables below for the new SAML Identity Provider object.

Parameter	Description	For More Information
General		
IdP Type	Select the type of the identity provider: <ul style="list-style-type: none">■ Microsoft AD FS - Microsoft Active Directory Federation Services■ Generic SAML - Another SAML-capable identity provider, such as Okta NOTE: The selected identity provider type cannot be changed afterwards.	
Configuration Mode	If you want to configure the identity provider information later on, select Fill in IdP details later (relevant if this application has not yet been configured in the identity provider)	
Active	Defines whether or not this provider is available at logon time	

Parameter	Description	For More Information
Service Provider Details		
Host Name	The URL address of the Provider and the port through which this server communicates.	
Port	The port is configurable and must be explicitly entered. The default value is 9000.	
Metadata (hidden by default)		



Parameter	Description	For More Information
Issuer	A unique identifier provided by the identity provider. This value is part of the service provider metadata. It is based on the Host Name value, but you can change it to a different value if necessary	See section 4.5.4.3 "Identity Provider (IdP) Requirements"
Callback URL	The URL that the browser is redirected to by the identity provider after successful authentication	
Logout URL	The identity provider redirects the user to this URL when they log out of the session. If logout is initiated from Threat Isolation, the identity provider is also notified to delete any cookies that the session has completed by calling the identity provider's logout URL	
Certificate	A certificate file used to secure communication with the service provider. Browse to upload the .pem file	

Parameter	Description	For More Information
Identity Provider Details - Do one of the following: <ul style="list-style-type: none">■ Click Import to populate the fields automatically. Select the relevant option:<ul style="list-style-type: none">◆ From URL... - Change the suggested URL to your SAML identity provider metadata URL◆ From file on computer - Provide a metadata file■ Specify the information manually, as described below.		
Entrypoint URL	The FQDN web address of the identity provider. This address is provided by the identity provider.	
Logout URL	Redirects the user to this URL when they log out of the session.	
Signing Certificate	Certificate file used for trusting assertions made by the identity provider. Browse to upload the .pem file.	

Parameter	Description	For More Information
Claims - The fields are displayed with their recommended values automatically.		
Username Attribute	The user attribute in the assertion that the identity provider returns on successful authentication	nameID Make sure to create a Claim Rule in the SAML IdP Configuration to map between "SAML Account Name" and "Name ID".



Parameter	Description	For More Information
Username Identifier Format	The user value format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
Groups Attribute	The group attribute in the assertion that the identity provider returns on successful authentication	http://schemas.xmlsoap.org/claims/Group Make sure to create a Claim Rule in SAML IdP Configuration to map between "Token-Groups - Unqualified Names" and "Group"

Parameter	Description	For More Information
Advanced		
Advanced Settings	Click Edit to display advanced settings	

4. Under Advanced settings, set the following values:
 - ◆ force_saml_auth default value is checked. If the value is unchecked, the identity provider will add a cookie in the user's browser to remove the requirement to log in to the IdP every time.
 - ◆ allow_saml_slo default value is unchecked. If the value is checked, once you log out of the system, you will be logged out of the identity provider and all the other 3rd party applications that integrate with the same IdP.

Click Update.

5. Click Create; the SAML Identity Provider is created.

4.6.3 Management Roles

Management roles define the various types of Management users and their access permissions (read/write or read-only) to the capabilities of Symantec Threat Isolation Management. These roles are provided out of the box and cannot be changed.



The Management capabilities are:

- Policy
- Management Users – Management roles, Management users and identity providers
- System Activity – Event logs, Management audit logs and Gateways audit logs
- End-user Activity – Activity logs, analytics

The following Management roles are provided:

Management Role	Has read/write (RW) or read-only (R) access to the building blocks:			
	Policy	Management Users	System Activity	End-user Activity
Administrator	RW	RW	RW	RW
Policy Editor	RW		RW	
Global Viewer	R	R	R	R
Policy Viewer	R		R	
Management Users Viewer		R		
System Activity Viewer			R	
End-user Activity Viewer				R

4.6.3.1 Assigning Members to Management Roles

You can assign Management users (members) to Management roles.

Note

- A Management user must be assigned to at least one Management role to be able to login to the system.
- A Management user can be assigned to more than one Management role.
- For internal authentication, Management users can be assigned to Management roles from the Management Roles page as well as from the Management User object. For more information, see section [4.6.1 "Creating Management Users"](#).

1. To assign a Management user (member) to a Management role, go to:
Management → Management Roles
2. Under Actions, click the edit icon for the relevant role.



3. If you have defined RADIUS Identity Provider objects, under Members, select the relevant option from the Provider drop-down list:
 - ◆ Internal Authentication (default)
 - ◆ RADIUS Server
 - ◆ SAML Identity Provider
4. Define the following parameters:

Parameter	Description	For More Information
For Internal Authentication		
Member	Specify the Management user to be assigned to this role	
For RADIUS Server		
Key	Specify the RADIUS server criterion key (the name of the attribute against which its value will be matched). Only use keys with values that are strings or numbers, not octets.	See section 4.6.2.1 "Creating RADIUS Identity Providers"
Value	Specify the RADIUS server criterion key value (the expected value of the attribute above). NOTE: In case of multiple keys and values, the relationship between them is OR.	
For SAML Identity Provider		
Attribute Type	Specify whether the Attribute type is Username, Group or Custom.	See section 4.6.2.2 "Creating SAML Identity Providers"
Claim (for Custom)	Specify the SAML Identity Provider criterion key (the name of the attribute against which its value will be matched).	
Value	Specify the SAML Identity Provider criterion key value (the expected value of the attribute above). NOTE: In case of multiple claims and values, the relationship between them is OR.	

5. Click Add.
6. Click Update to save the updated Management role.



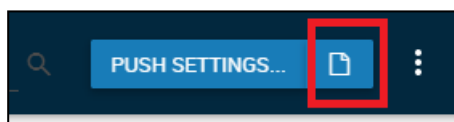
4.6.4 Viewing Management Audit Logs

Audit log records are maintained on all actions performed in the Symantec Threat Isolation Management UI. The logs can be forwarded using log forwarding (see section [6.4 "Log Forwarding"](#)).

Note

Management audit log functionality requires a Report Server to be defined. See section [6.3 "Defining a Report Server"](#), and [3.5.7 "Defining the Management Gateway"](#), Step 12, for enabling the Report Server.

- To view the Management Audit Log, do one of the following:
 - ◆ Go to:
Management → Management Audit Log
 - ◆ Click the Audit Log button at the top right of the screen, beside the Push Settings button.




Note


- When no changes need to be pushed to the Threat Isolation Gateways, the Audit Log button is displayed as follows:
- When changes are ready to be pushed to the Gateways, the button is displayed as follows: Click the button to view all Management audit log records awaiting Push Settings. For more information, see section [4.7.6 "Pushing Settings"](#)

The following table describes the Management Audit Log parameters.

Parameter	Description	For More Information
# (Number)	A unique number assigned to each log item	
Timestamp	The date and time of the event	



Parameter	Description	For More Information
Settings Version	<p>A unique number assigned to every version.</p> <p>Each version is created when the Push Settings button is clicked. When an action requires a push to send the version update to the system, the  icon is displayed beside the version number. This indicates that changes will be pushed to the Gateways the next time Push Settings is performed</p>	
User	The Management user who initiated the log event	
Action	<p>The change that occurred to trigger the log event.</p> <p>An action is one of the following:</p> <ul style="list-style-type: none">■ Login /Failed Login■ Create■ Update■ Delete■ Push Settings	
Object Type	The type of object that was changed	
Description	A description of the event	

- To refresh the Management Audit Log, click the  icon at the top right of the screen.
- To view a detailed description of an audit log, click its line number or timestamp. Additional information is displayed by selecting Object View in the detailed description of the audit log, with the following actions:

Action	Object View Display
Create	Displays the newly added data for the object creation
Update	Displays the before and after modification
Delete	Displays the data that has been deleted



4.7 Defining Zones, Gateways, and Associated Components

The main topics in this section include:

- [System Security Policy Distribution Hierarchy](#)
- [Configuring the Zone](#)
- [Defining a Threat Isolation Gateway](#)
- [Defining Gateway Advanced Settings](#)
- [Defining Gateway Clusters](#)

4.7.1 System Security Policy Distribution Hierarchy

The following diagram illustrates the hierarchy of the Symantec Threat Isolation system security policy distribution.

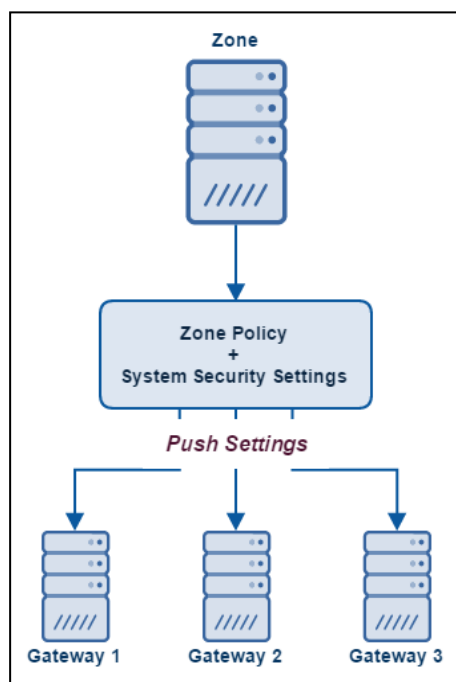


Figure 12 Symantec Threat Isolation System Security Policy Distribution Hierarchy



4.7.2 Configuring the Zone

4.7.2.1 Overview

In the Symantec Threat Isolation system, the Zone represents a server farm made up of multiple Threat Isolation Gateways that share the same Proxy Auto-Configuration (PAC) file and CA certificate. The Zone has a single security policy defined for it, which consists of a policy rule base – a number of policy rules that are enforced on a first-match basis – and system configuration parameters, as described in section [4.2 "Defining Security Policies and Rules"](#). The Push Settings function distributes the Zone's policy to all Gateways associated with the Zone.

In the future, it might be possible to define multiple zones. Then, each Zone would maintain a separate security policy, and the Push Settings function would distribute each Zone's policy to that Zone's associated Gateways. For example, designating multiple zones would enable organizations to define separate zones for its branches that reside on different local area networks (LANs). As well, multinational organizations would be able to define a separate Zone for each country in which they have offices, with separate policies and rules tailored to each country's security regulations and organizational requirements.

Currently, Symantec Threat Isolation supports a single Zone, the default Primary Zone, which is available out of the box.

Zone settings define the security policy assigned to the Zone and the CA certificate associated with the Zone. The settings enable you to update the Zone's Affinity rules for routing specific source IPs to specific Threat Isolation Engines (TIEs) (see section [4.7.2.3 "Updating Threat Isolation Engine Affinity"](#)), and to update its PAC file settings, which instruct web browsers and user agents how to choose the appropriate proxy server for fetching URLs. Note that a PAC file is generated automatically for the Zone (for more information, see section [4.7.2.4 "Updating a Zone's PAC File"](#)).

Zone settings are applied from the physical location of clusters. For information about clusters, see section [4.7.12 "Defining Gateway Clusters"](#).

4.7.2.2 Defining the Zone

1. To define the Zone, go to:
`System Configuration → Zones`
2. Under Actions, click the edit icon.
3. Define the parameters described in the table below, and then click Update.



Parameter	Description	For More Information
General		
Policy	Security policy assigned to the Zone	See section 4.2 " Defining Security Policies and Rules "
CA Certificate	The CA certificate associated with the Zone: <ul style="list-style-type: none">■ A custom CA certificate that was imported into the system (good practice)■ The default CA certificate that Symantec Threat Isolation supplies out of the box (recommended only for demo purposes)	See sections 3.4.4 " Signing the CA Certificate " and 4.8 " Configuring System Certificates "
Advanced		
Threat Isolation Engine Affinity	<ul style="list-style-type: none">■ Enables mapping between source addresses and TIEs■ When affinity is enabled, web browsing becomes more efficient. For example, when an end user browses to a website, all of its tabs will be mapped to the same Threat Isolation Engine (TIE). Note that affinity rules are not effective in the case of endpoints behind a NAT	See section 4.7.2.3 " Updating Threat Isolation Engine Affinity "

4.7.2.3 Updating Threat Isolation Engine Affinity

You can map traffic from endpoint-designated networks to specific Threat Isolation Engines (TIEs).



1. To update TIE affinity, in the Update Zone window, under Threat Isolation Engine Affinity, click Edit.

2. Click Add Rule.
3. Define the Traffic Mapping Policy parameters, described in the table below.

Parameter	Description	For More Information
Rule name	<ul style="list-style-type: none">■ Default rule is the one available with Symantec Threat Isolation out of the box■ Click Add rule to add a new rule to the list.	
Source	IP-based network object, such as: <ul style="list-style-type: none">■ IP address■ IP range■ Subnet/Mask	See section 4.4.6.2 "Creating a Custom Read-Only Page"
Threat Isolation Engines	TIEs affected by this rule	See section 4.7.9 "Defining Threat Isolation Engines (TIEs)"
Description	Description of the rule	

4. When you have made your changes, close the Update Threat Isolation Engine Affinity window.
5. Click Update in the Update Zone window to save your changes.

**Note**

Affinity rules are not effective when endpoints are behind a NAT. All endpoints behind a NAT have the same source IP and therefore cannot be identified by their IP address.

4.7.2.4 Updating a Zone's PAC File

A Zone's Proxy Auto-Configuration (PAC) file is an automatically-generated file that defines this specific Zone's configuration. It instructs web browsers and user agents on how to choose the appropriate proxy server for fetching URLs. You can view the PAC file in your Zone settings.

The auto-generate feature associated with the PAC file ensures that any changes in your Symantec Threat Isolation security policies and their settings are automatically added to the PAC file. This means that the browser will choose the correct Threat Isolation Proxy or Threat Isolation Engine (TIE) with every URL requested.



Disabling the auto-generate feature for your Zone's PAC file enables you to edit the file manually. However, this turns the PAC file into a customized file whose changes to the Symantec Threat Isolation security policy are not reflected in the Zone's existing PAC file.

Note

Manual changes to the PAC file might result in unexpected system behavior. Do not make any manual changes to a PAC file without first consulting Symantec Threat Isolation technical support.

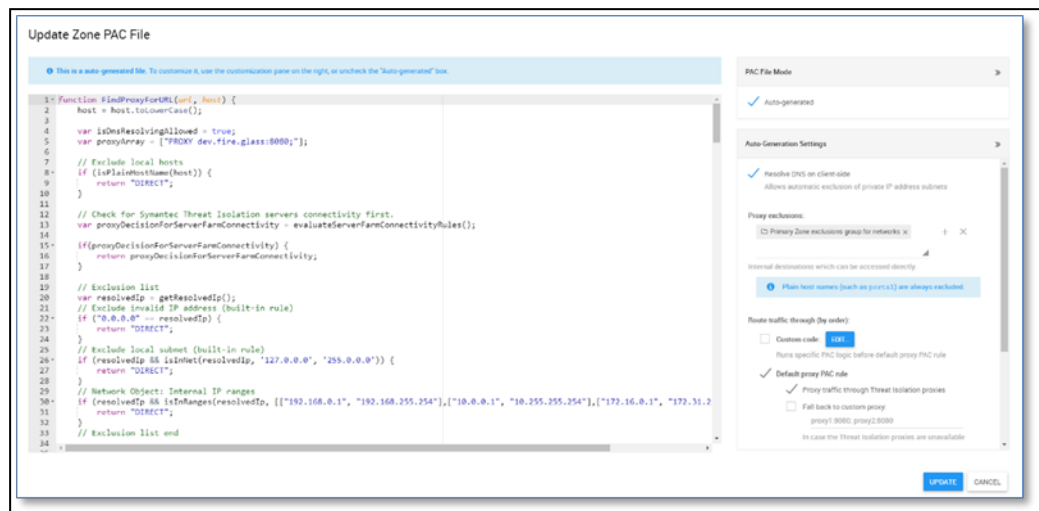
1. To access the PAC file, go to:

System Configuration → Zones → Edit PAC File

Zones <small>View or edit Zones</small>				
Name	Policy	Description	Updated At	Actions
Primary Zone	My Policy	(System created)	17 minutes ago	 



The Update Zone PAC File window is displayed.



2. Do one of the following:

- ◆ (Recommended) Keep the Auto-generated checkbox selected - Symantec Threat Isolation maintains the PAC file. This ensures that any changes you make in the Custom code UI control will be added to the PAC file automatically.
- ◆ (Recommended only for changes in areas that are not affected by Custom code control) Clear the Auto-generated checkbox - Allows you to edit the PAC file manually, but turns it into a customized file that Symantec Threat Isolation no longer maintains. Changes in the PAC parameters described below will be reflected only after clicking Regenerate Now.

Note that when you click Regenerate Now, any PAC content that was changed in the text area will be overridden by the new UI and needs to be changed again in the newly-generated file. If you want Symantec Threat Isolation's logic to be incorporated in your customized file, you will need to merge it with your customized file manually, for example by using a data comparison tool.

3. Edit the PAC file parameters, described in the table below.

Parameter	Description	For More Information
Auto-Generation Settings		



Parameter	Description	For More Information
Resolve DNS on client side	Select to allow automatic exclusion of private IP address subnets	
Proxy exclusions	Add the internal destinations that can be accessed directly. Note that plain host names (such as “portal”) are always excluded	
Route traffic through (by order) - The following three parameters will be run by their order:		
Custom code	Add specific PAC rules that will run before the default proxy PAC rule. When this parameter is selected, click Edit to add custom code. The custom code will be added between the following code text: CUSTOM_PAC_LOGIN_BEGIN, CUSTOM_PAC_LOGIC_END.	
Default proxy PAC rule	The default proxy rule that runs at the end of the PAC file logic. Choose the relevant option(s): <ul style="list-style-type: none">■ Proxy traffic through Threat Isolation proxies■ Fall back to custom proxy when Threat Isolation Proxies are unavailable■ Fall back to direct access when both of the above fail	
Default TIE PAC rule	The default TIE rule that runs at the end of the PAC file logic. Choose the relevant option(s): <ul style="list-style-type: none">■ Proxy TIE traffic through custom proxy■ Fall back to custom proxy when the above fails	

4. (Relevant only if the Auto-generated checkbox is clear) Click Regenerate Now to reflect the UI control changes.

Note

Any PAC content that was changed in the text area will be overridden by the new UI and needs to be changed again in the regenerated file.

5. To route traffic through a proxy that is not the Threat Isolation Proxy, clear Default proxy PAC rule, and select the checkbox next to Custom Code.
6. Click Edit to open the Custom Code Editor and define the new proxy through which the traffic will be routed.



Custom Code Editor

```
1 // Sample code (you can use any PAC file function here):
2 // if(resolvedIp == '127.0.0.1') {
3 //     return "DIRECT";
4 // }
5 // If you do not return any value here, the Symantec Threat Isolation Proxy will
```

UPDATE CANCEL

7. Click Update to add your custom code to the PAC file.

Your code is added at the end of the PAC file code flow, in the area highlighted in the following image.

Update Zone PAC File

This is a auto-generated file. To customize it, use the customization pane on the right, or uncheck the "Auto-generated" box.

```
18 // Exclusion list
19 var resolvedIp = getResolvedIp();
20 // Exclude local IP address (built-in rule)
21 if ("0.0.0.0" == resolvedIp) {
22     return "DIRECT";
23 }
24 // Exclude local subnet (built-in rule)
25 if (resolvedIp && isSubnet(resolvedIp, "127.0.0.0", "255.0.0.0")) {
26     return "DIRECT";
27 }
28 // Network Object: Internal IP ranges
29 if (resolvedIp && isInRange(resolvedIp, [{"192.168.0.1", "192.168.255.254"}, {"10.0.0.1", "10.255.255.254"}, {"172.16.0.1", "172.31.255.254"}])) {
30     return "DIRECT";
31 }
32 // Exclusion list end
33
34 //PG-CUSTOM_PAC_LOGIC_BEGIN
35 //PG-CUSTOM_PAC_LOGIC_END
36
37 return "PROXY dev.fire.glass:8080";
38 // PAC file logic ends here.
39
40 // Helper code:
41 function evaluateForConnectivityRules() {
42     // Symantec Threat Isolation servers connectivity
43     if (shExpMatch(url, "http://dev.fire.glass:3000/test_pages")) {
44         return "PROXY dev.fire.glass:8080";
45     }
46     if (shExpMatch(url, "http://dev.fire.glass:3000/recorder")) {
47         return "DIRECT";
48     }
49     if (shExpMatch(url, "http://dev.fire.glass:3000/recorder")) {
50         return "DIRECT";
51     }
52     if (shExpMatch(url, "http://dev.fire.glass:3000/recorder")) {
53         return "DIRECT";
54     }
55 }
```

PAC File Mode

☒ Auto-generated

Auto-Generation Settings

☒ Resolve DNS on client side
Allows automatic exclusion of private IP address subnets

Proxy exclusions

☐ Primary Zone exclusions group for networks at: + X

Internal destinations which can be accessed directly

☒ Then host names (such as port44) are always excluded.

Route traffic through (by order):

☐ Custom code: [View...](#)

☒ Default proxy PAC rule

☒ Proxy traffic through Threat Isolation proxies

☐ Fall back to custom proxy group1:8080, proxy2:8080

In case the Threat Isolation proxies are unavailable

UPDATE CANCEL

8. Click Update in the Update Zone PAC File dialog.
9. Click Push Settings to add the changes to the Zone's PAC file.

**Notes**

- When you add a new Gateway from the Gateways window in the Symantec Threat Isolation Management UI, the new Gateway is reflected automatically in new lines of code in the automatically-generated PAC file.
- When you add a new Gateway by changing the PAC file manually, the new Gateway is *not* added to the Gateways window.

4.7.3 Understanding the Threat Isolation Gateway and Its Components

- As part of the system configuration, you can create one or more Threat Isolation Gateways and Policy Distribution Points (PDPs), Threat Isolation Engines (TIEs), and Threat Isolation Proxies, each on a separate physical server.
- Each Gateway can include a Proxy, a TIE, or both, but no more than one of each.
- The Gateway can be connected to the Internet, to Active Directory (AD), or to other servers.
- A Gateway that has the TIE enabled will typically be connected to the Internet, since the TIE is responsible for isolation.
 - ◆ A Gateway that has a Proxy enabled will typically be connected to the AD, since the Proxy is responsible for authentication.
- The PDP (a logical component) resides on one of the Gateways. The PDP is responsible for communication with the TIEs (for more information, see section [2.4 "Platform Components"](#)). **Important:** If the PDP is enabled on a Proxy Gateway, the TIE Gateways will have to access the Proxy. To avoid this, for security best practice it is recommended to enable the PDP on a TIE Gateway.

For more information about Symantec Threat Isolation components, see sections [2.4 "Platform Components"](#) and [4.7.1 "System Security Policy Distribution Hierarchy"](#).

4.7.4 Selecting the Policy Distribution Point (PDP)

For information about how to select a Policy Distribution Point (PDP) for a Threat Isolation Gateway, see section [4.7.7 "Defining a Threat Isolation Gateway"](#). For general information about the PDP, see section [2.4 "Platform Components"](#).



4.7.5 Understanding the Gateway Settings Table

- To access the Gateway settings page, go to:

System Configuration → Gateways

The Gateway settings table provides the following information.

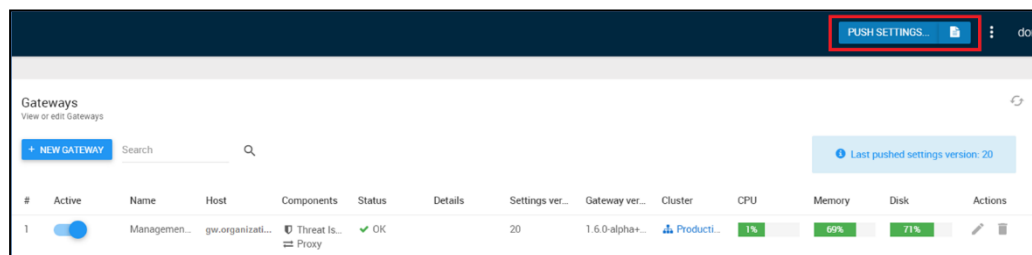
Column	Description	For More Information
Active	Whether the Gateway is functioning	
Name	Gateway name	
Host	DNS for this Gateway	
Components	Components running on this Gateway. Can be one or more of the following: <ul style="list-style-type: none">■ Threat Isolation Engine (TIE)■ Threat Isolation Proxy	
Status	Gateway status. Can be one of the following: <ul style="list-style-type: none">■ Unregistered. The Gateway registration key has not yet been used during the Gateway installation process■ Uninitialized. This Gateway has not yet undergone the initialization process■ OK. The Gateway is functioning as expected■ Error. If an error has occurred, it is described in the Details column■ Disconnected. The Gateway is disconnected■ Pushing Settings. This status occurs during the Push Settings process	
Details	Detailed information about the error noted in the Status column	
Settings Version	The most updated policy version is displayed above the Gateway table.	
Gateway Version	Version pertaining to Gateway entry	



Column	Description	For More Information
Cluster	One of the following, or another cluster you define: <ul style="list-style-type: none">■ Production■ Staging	
Monitoring Settings		
CPU	Current CPU usage, as %	
Memory	Current memory usage, as %	
Disk	Current disk usage, as %	
The three values above refresh automatically every 10 seconds and provide basic system monitoring information per Gateway. The values are color-coded, as follows: <ul style="list-style-type: none">■ Green - less than 70%■ Yellow - 70% to 84%■ Red - 85% and above		

4.7.6 Pushing Settings

The Push Settings button is available from any location in the UI and always appears on the right-hand side of the top bar, as shown below.



- When setting updates should be pushed to the Gateways, the following icon is displayed:



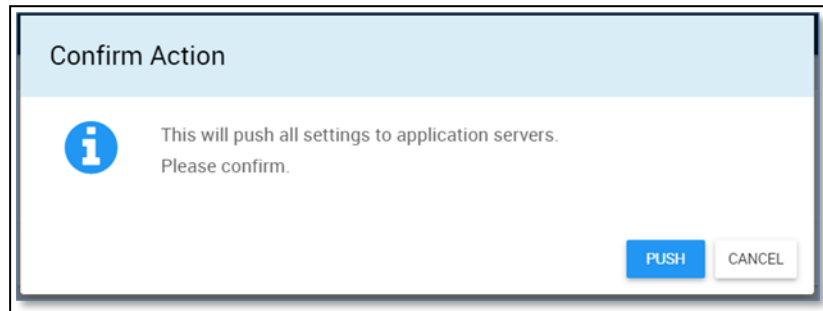
- When there are no setting updates to be pushed to the Gateways, the following icon is displayed:





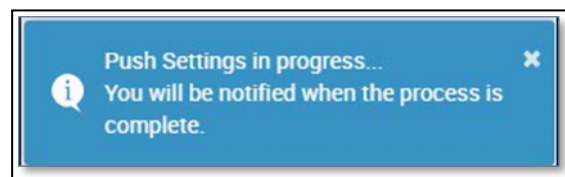
The Push Settings button deploys the current settings to all Gateways (Threat Isolation Proxies and TIEs). During the push settings process, the status "Pushing Settings" appears in the Status column for the affected Gateways.

1. Click Push Settings.



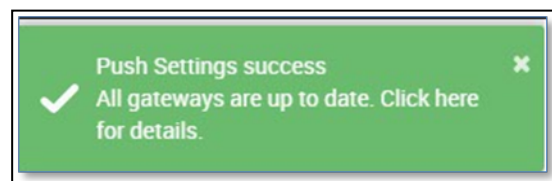
2. Click Push to confirm the Push Settings action.

A progress bar appears. When it disappears, a message appears in the lower-right corner of the Gateways window.



You can continue working in the Management area and navigate between pages while the settings are being pushed.

After the push settings process has completed, a following confirmation message appears in the lower-right corner of the Gateways page.



- ◆ For all Gateways that received the new settings successfully, the Last Settings Version is incremented.
- ◆ The Settings version value is also incremented for every Gateway that the policy has reached successfully.



4.7.7 Defining a Threat Isolation Gateway

A Threat Isolation Gateway contains one or more Threat Isolation Engine (TIE) and Threat Isolation Proxy components. The Gateway is the minimum physical component on which these various logical components can run. For more information, see section [2.4 "Platform Components"](#).

Note

Symantec Threat Isolation supports scaling; as more end users are added to your organization, more Gateways can be added. Scaling is also supported for high availability and load balancing.

1. To create a Threat Isolation Gateway, go to:
System Configuration → Gateways → New Gateway
2. Configure the parameters described in the table below for the new Gateway.

Parameter	Description	For More Information
General		
Name	Unique name you assign to this Gateway	
Host	Host name with which this Gateway is associated For each Gateway's Host, enter its FQDN that was defined as part of the networking preparation for installation	See section 3.4.3 "Defining Networking"
Public DNS Name	A DNS-resolvable name for the client computer (optional) If the Public DNS Name is configured, the browser will regard the Public DNS Name value as the effective host If no value is configured, the browser will regard the Host as the effective machine host	See section 4.7.7.2 "Enabling Web Application Isolation Gateway Mode with a Load Balancer" , and "Configuring the Public DNS Name"
Location		



Parameter	Description	For More Information
Zone	<ul style="list-style-type: none">■ Designates the server farm to which this Gateway is assigned■ Currently, Symantec Threat Isolation supports only a single Zone, the default Primary Zone. When you define a new Gateway, it is assigned to the Primary Zone by default■ Load balancing of the system's Gateways is handled by the PAC file, based on the priority defined for each Gateway	
Cluster	<p>Add the Gateway to one of the following clusters, or to any other cluster you define:</p> <ul style="list-style-type: none">■ Production■ Staging	
Components		
Components	<p>Component(s) running on the Gateway:</p> <ul style="list-style-type: none">■ Threat Isolation Proxy■ Threat Isolation Engine (TIE)	
<p>Certificates - The Threat Isolation Gateway must have a server certificate to allow a secure connection to be established between the Gateway and the browser. Multiple Gateways with the same Public DNS name can share a single server certificate object.</p> <p>Select the server certificate that the new Gateway will use:</p>		
Server Certificate	<ul style="list-style-type: none">■ The auto-generated server certificate signed by the Zone CA, or■ A custom server certificate that you have imported into the system	See section 4.8 "Configuring System Certificates" 4.8 "Configuring System Certificates"
<p>Access - You can define the Symantec Threat Isolation Platform as being connected to one or more of the following:</p>		
DNS	<ul style="list-style-type: none">■ Access to DNS server■ In case of no access, DNS resolution is forwarded to next hop proxy/server	



Parameter	Description	For More Information
Next Hop Proxy/Server	URL for next hop proxy/server between the Gateway and the Internet Note that changing the next hop proxy/server setting requires a service restart on the Gateway machine	See sections 4.7.7.1 "Configuring a Next Hop Proxy/Server" and 4.10 "Integrating a Downstream Proxy"
NTP Servers	<ul style="list-style-type: none">■ Allows automatic NTP time synchronization■ If NTP is enabled, add the NTP server list	
Internet	Internet access for this Gateway. If this Gateway has no Internet access: <ul style="list-style-type: none">■ URL categorization information is automatically retrieved from other Gateways that have an Internet connection■ Pass rules are not supported	
Active Directory	AD access for this Gateway It is common practice to maintain the highest level of security for the AD and ensure that any server connected to it resides within the organization's LAN behind the firewall	See section 4.5.2 "Defining Active Directory Settings"
Remote Support	Select to allow Symantec support access to the Gateway machine's command line interface	
Active Directory Authentication		



Parameter	Description	For More Information
Keytab	<p>The Keytab objects that are assigned to this Gateway's Public DNS name</p> <ul style="list-style-type: none">■ Active Directory Access must be selected■ The Gateway Public DNS Name field or the Gateway Host field must be defined before the Keytab can be assigned to the Gateway■ The Public DNS Name and/or Host name must be identical in spelling to the name of the Keytab machine <div>Note Selecting Active Directory Access without assigning a Keytab to the Gateway's Public DNS name is not recommended and will default to NTLM, which is considered a weak authentication protocol.</div>	See section 4.5.3 "Creating Keytab Settings" for Keytab setup
SNMP Settings		
Expose system metrics	<p>Select to allow the Gateway to expose system metrics on demand in response to a SNMP Walk/GET request sent by the SNMP server</p> <p>NOTE: The Gateway's response to a SNMP Walk/GET request by the SNMP server contains only system metrics</p>	For information about how the Management server sends system metrics and application metrics to the SNMP server when a metrics threshold is crossed, see section 4.13 "Configuring SNMP Servers"
Community Name	<p>String used to authenticate SNMP requests. Default: "public"</p> <p>When the community name is edited, its new value will be the default when a Gateway is created</p> <p>NOTE: This field is only enabled when Expose system metrics is selected, above</p>	
SAML Authentication		
Settings	Select the appropriate SAML object	See section 4.5.4 "Defining SAML Trust"



Parameter	Description	For More Information
Status (relevant only when editing or deleting a Gateway object)		
Status	Gateway operation status	
IP	The egress IP of the Gateway	
Advanced parameters		
Advanced Settings	Selects a Gateway Advanced Settings object. This object enables defining the Gateway for the Web Application Isolation Gateway Mode topology	See section 4.7.8 "Defining Gateway Advanced Settings"
Debug Level	<p>One of the following:</p> <ul style="list-style-type: none">■ Error■ Warn■ Info■ Debug■ Trace■ Default - The Gateway decides the debug level on a per-component basis <p>All values other than "Default" override the default value defined on this Gateway</p>	
Use this Gateway as a passive failover	<p>Select to prevent Management from showing an error in the Gateways page when this Gateway is not responding</p> <p>It is good practice to select this checkbox when the Gateway is intentionally down due to a failover</p>	



3. Click Create.

The New Gateway Registration screen is displayed.

4. In the Security Policy section, select the Policy Distribution Point (PDP) for this Gateway from the following options:
 - ◆ The Gateway is the PDP: The PDP will be enabled on the Gateway that you are now defining.

IMPORTANT!

By default, the PDP will reside on the first Gateway that you register. If the PDP is enabled on a Threat Isolation Proxy Gateway, the Threat Isolation Engine (TIE) Gateways will have to access the Threat Isolation Proxy. To avoid this, for security best practice it is recommended to enable the PDP on a TIE Gateway.

- ◆ The current Gateway will connect to the PDP that resides on the Gateway you select from the drop-down list.
 - ◆ Decide later. Note that as long as the Gateway is not registered, it will not be part of the Zone's policy.
5. In the Registration Instructions section, copy the registration command.



This command is required input in the Gateway initialization interface during the installation process. For information about the Gateway initialization process, see section [3.5.9 "Initializing Gateways"](#).

Note

For as long as the Gateway is not registered, you can return to the New Gateway Registration screen by clicking the key icon for this Gateway under Actions in the Gateways page. You can then copy the registration command and use it in the Gateway initialization process.

6. Click OK to complete the procedure.

4.7.7.1 Configuring a Next Hop Proxy/Server

When the Threat Isolation Engine (TIE) communicates indirectly with the Internet, you might be required to configure the proxy that acts as a go-between.

The next hop proxy/server resides between the Threat Isolation Proxy and the Internet, and can be one of the following:

- Transparent proxy – If the proxy is transparent, routing through the proxy is automatic and no configuration is required.
- Explicit proxy – For explicit proxies, you need to define the proxy settings as described in section [4.11 "Creating New Next Hop Proxy/Server Settings"](#).

4.7.7.2 Enabling Web Application Isolation Gateway Mode with a Load Balancer

The Web Application Isolation mode protects an organization's applications from attack. For more information, see section [2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode"](#).

In Web Application Isolation mode with a load balancer, all end user browser communication is done through a third-party load balancer that distributes traffic among multiple Threat Isolation Gateways sharing the same DNS name.

To enable Web Application Isolation mode:

1. Click the label of the Gateway Advanced Setting object (see section [4.7.8 "Defining Gateway Advanced Settings"](#)).
2. Under Portal Settings, select Enabled.
3. Make sure the Show address bar is clear.
4. In the Home page field, specify the address of the web application to be protected. This address will be loaded as the Home page.
5. Click Update.

**Note**

In Components, make sure that only the Threat Isolation Engine (TIE) component is selected.

Configuring the Public DNS Name**Note**

Web Application Isolation mode is useful when your organization uses an external load balancer. In this mode, WebSocket communication to the TIE should be done via its Public DNS. The load balancer, which must support WebSocket, distributes traffic among multiple Gateways.

1. In Components, under the TIE component, choose the Public DNS Name responsible for handling WebSocket communication:

Set the Public DNS name of the TIE to the DNS name of the load balancer by changing the default (Host) to DNS name.
2. Click Update.

Adding a Server Certificate

This Gateway and all others use the same Public DNS name. Therefore, the server certificate needs to be issued to one hostname (the Public DNS Name of the load balancer).

1. Outside of the Symantec Threat Isolation Platform, create a server certificate object that includes the generated certificate. For more information, see section [4.8.2 "System Server Certificates"](#).
2. Under Server Certificates, select the second option: Use a custom server certificate.
3. Select the custom server certificate object.

Notes

- Make sure the server certificate is signed by a CA that your endpoints already trust: Either your organizational root CA, or a root CA that is a trusted by the trusted certificate authorities of the Operating System.
- If your organization wants to sign the certificate itself, but no organizational CA exists, create a CA certificate (see section [3.4.4.3 "Signing the CA Certificate File"](#)) and then deploy it (see section [3.5.11 "Installing the CA Certificate as Trusted Root CA on the Client Side"](#)) (less recommended).



Configuring a Load Balancer Health Check

When the application is isolated behind a load balancer, it is recommended to configure a health check with the following settings:

- Protocol: HTTPS
- The portal host: 443
- Path: /portal_index.html
- Success code: 200. Otherwise, failure

Note

If all health checks fail, for connectivity it is recommended to configure a fallback that makes the load balancer direct traffic to the original application website.

Authentication

- Web Application Isolation mode does not include a proxy component responsible for authentication. Instead, the TIE is responsible for authentication. For more information, see section [2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode"](#).

Note

Only for AD authentication in Web Application Isolation mode, the TIE requires connection to Active Directory in addition to Internet connection. (This is not relevant for SAML authentication.)

Link Isolation URL

- In Web Application Isolation mode, all end user browser communication with the Internet is routed through a specific URL for the Gateway that has been designated for use as a reverse proxy.
- For end user webpage requests, Web Application Isolation mode is designated in the endpoint browser by the URL.

For example:

The requested URL in the Web Application Isolation address bar is:

`https://www.google.com`



When the public DNS of Web Application Isolation is `web-application-protection.myorganization`, and the requested URL in the Web Application Isolation address bar is `https://www.google.com`, then the URL that the browser will request, will be:

```
https:// web-application-  
protection.myorganization.com/?url=https://www.google.com
```

Note that the Web Application Isolation DNS name is the DNS of the load balancer.

Client Side Setup

When the certificate is signed by a root CA that your endpoints already trust, no special setup is required at the client side.

4.7.8 Defining Gateway Advanced Settings

1. To access the Gateway Advanced Settings, go to:
`System Configuration → Gateway Advanced Settings`
2. Do one of the following:
 - ◆ Define new Gateway Advanced Settings, as follows:
 - When creating a Threat Isolation Gateway, click New Gateway Advanced Setting, or
 - Clone existing Gateway Advanced Settings (for more information, see section [4.3.2 "Cloning Objects"](#)).
 - ◆ Edit the default or existing Gateway Advanced Settings.
3. Configure the parameters described in the following table.

Parameter	Description	For More Information
Portal		



Parameter	Description	For More Information
Portal Settings	<ul style="list-style-type: none">■ Enabled - Enables the Web Application Isolation Gateway. Must be selected for the following topologies:<ul style="list-style-type: none">◆ Block Page Integration◆ Symantec Email Threat Isolation◆ Web Application Isolation Gateway Mode■ Show address bar - Enables the portal address bar. Must be selected for the Portal Isolation Mode scenario. Must be clear for the following topologies:<ul style="list-style-type: none">◆ Block Page Integration◆ Symantec Email Threat Isolation◆ Web Application Isolation Gateway Mode■ Home page - Default URL isolated when accessing the portal.<ul style="list-style-type: none">◆ In the web application protection scenario, the address specified in this field is loaded as the home page. This page is static; the end user cannot choose to navigate to other web pages from it◆ In the portal isolation scenario, this address is the first isolated web page to be loaded	<ul style="list-style-type: none">■ See section 4.7.7 "Defining a Threat Isolation Gateway"■ See section 2.6.4 "Symantec Threat Isolation with Block Page Integration"■ See section 2.6.5 "Symantec Email Threat Isolation"■ See section 2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode"■ See section 4.7.8.2 "Portal Isolation Mode"
Feedback Email Settings		
Feedback Email Settings	<ul style="list-style-type: none">■ Send feedback emails - Enables the option to send email feedback■ Send Via - Enables the Symantec Threat Isolation cloud email server or an admin-defined internal email server■ Send To - Specify an email address where feedback emails are delivered. Additionally, you can accept the Symantec Threat Isolation support email	
Advanced		
Internal Settings	<p>Click Edit to see internal Gateway settings.</p> <p>WARNING: Changing these internal settings can result in unexpected system behavior. Contact Symantec Threat Isolation technical support for assistance.</p>	



4.7.8.1 Enabling Web Application Isolation Gateway Mode - No Load Balancer

The Web Application Isolation mode protects an organization's applications from attack. For more information, see section [2.6.6 "Symantec Threat Isolation as Web Application Isolation Gateway Mode"](#).

To enable Web Application Isolation mode:

1. Click the label of the Gateway Advanced Setting object.
2. Under Portal Settings, select Enabled.
3. Make sure the Show address bar is clear.
4. In the Home page field, specify the address of the web application to be protected. This address will be loaded as the Home page.
5. Click Update.

Note

In Components, make sure that only the Threat Isolation Engine (TIE) component is selected.

Adding a Server Certificate

Note

In a Web Application Isolation scenario without a load balancer, where multiple Threat Isolation Gateways share the same DNS name, for stickiness purposes the TIEs listen to WebSocket requests by their unique hostname rather than the Public DNS name.

For simple deployment, it is good practice to provide a single server certificate, saving you from having to supply a key pair to each Gateway individually. The certificate must include both the Public DNS name (for the initial connection) and the hostnames of all involved Gateways (for WebSocket requests).



When adding a server certificate, you have the following options.

■ Wildcard certificate

If your Gateways have different names (for example, tie-1, tie-2, ...) but share the same domain (for example, myorganization.com) and Public DNS name (for example, web-application-protection.myorganization.com), you can generate a wildcard certificate. In a wildcard certificate, the subject is represented by * followed by the domain. For example, a wildcard certificate can be issued to:

`*.myorganization.com`

Since the hostnames and Public DNS of your Gateways share the same domain, you will not need to regenerate the certificate when a new Gateway is added.

Notes

- Make sure the server certificate is signed by a CA that your endpoints already trust: Either your organizational root CA, or that of a commercially trusted root CA, such as Verisign.
- If your organization wants to sign the certificate itself, but no organizational CA exists, create a CA (see section [3.4.4.3 "Signing the CA Certificate File"](#)) and then deploy it (see section [3.5.11 "Installing the CA Certificate as Trusted Root CA on the Client Side"](#)) (less recommended).

■ Multi-Domain (SAN) Certificate

Unlike the flexible wildcard certificates, SAN certificates include an explicitly defined alternative name for each Gateway. This means that when a Gateway is added, the SAN certificate must be regenerated to include the name of the new Gateway.

For example, the following SAN fields will be used:

`tie-1.myorganization.com`

`tie-2.myorganization.com`

`tie-N.myorganization.com`

`web-application-protection.myorganization.com`



Authentication

- Web Application Isolation mode does not include a proxy component responsible for authentication. Instead, the TIE is responsible for authentication. For more information, see section [2.4 "Platform Components"](#).

Note

Only for AD authentication in Web Application Isolation mode, the TIE requires connection to Active Directory in addition to Internet connection. (This is not relevant for SAML authentication.)

Link Isolation URL

- In Web Application Isolation mode, all endpoint browser communication with the Internet is routed through a specific URL for the Gateway that has been designated for use as a reverse proxy.
- For end user webpage requests, Web Application Isolation mode is designated in the endpoint browser by the URL.

For example:

The requested URL in the Web Application Isolation address bar is:

`https://www.google.com`

When the public DNS of Web Application Isolation is `web-application-protection.myorganization.com`, and the requested URL in the Web Application Isolation address bar is `https://www.google.com`, then the URL that the browser will request, will be:

`https://web-application-protection.myorganization.com/?url=https://www.google.com`

Client Side Setup

When the certificate is signed by a root CA that your endpoints already trust, no special setup is required at the client side.

4.7.8.2 Portal Isolation Mode

In Portal Isolation mode, only the Threat Isolation Engine (TIE) component is active in the Symantec Threat Isolation Platform. In this scenario, the Threat Isolation Gateway functions as a Web Isolation portal, running an isolated website inside the native browser. Portal Isolation mode can be used to isolate websites in cases where the end user's proxy settings cannot be changed, to protect an organization's end users from attack.



GPO policy is not deployed to end users who are not part of the Active Directory domain. If the end users are not part of your organizational domain, make sure the Gateway's server certificate is signed by the root CA of an external vendor, such as VeriSign, that is trusted by all endpoints. Portal Isolation enables the isolation of such users who are not managed by the organization's network. Protection is also provided when end users use their own devices (Bring Your Own Device – BYOD) to access company websites, and when guests access the organization's guest Wi-Fi.

In Portal Isolation mode, all content requests from end users go through a single URL (the Home page) to a dedicated Gateway. From the Home page, end users can navigate to other isolated pages. This mode requires no configuration in the endpoint browser.

4.7.9 Defining Threat Isolation Engines (TIEs)

- You define each Threat Isolation Engine (TIE) when you define a Threat Isolation Gateway.
- You can define and configure multiple TIEs, but only one TIE can be associated with each Gateway.
- TIEs normally require a connection to the Internet. However, there is an exception that arises when dealing with application protection, where the web server that hosts the application resides on the LAN and is not connected to the Internet.
- Typically, the TIE resides in the DMZ, and does not require direct access to the organization's Active Directory.

See section [4.7.3 "Understanding the Threat Isolation Gateway and Its Components"](#), for a description of the Symantec Threat Isolation Platform definition and configuration process.

4.7.10 Defining Threat Isolation Proxies

- You define each Threat Isolation Proxy when you define a Threat Isolation Gateway.
- You can define and configure multiple Threat Isolation Proxies, but only one Threat Isolation Proxy can be associated with each Threat Isolation Gateway.
- Since the Threat Isolation Proxy performs end user authentication, it requires access to the organization's Active Directory.
- When a Threat Isolation Proxy is associated with a Threat Isolation Gateway, the hostname designated for the Gateway is replicated to the Zone's PAC file.



4.7.11 Defining a Web Application Isolation Gateway

- You define a Threat Isolation Gateway as a Web Application Isolation Gateway through the Gateway Advanced Settings, as described in section [4.7.7.2 "Enabling Web Application Isolation Gateway Mode with a Load Balancer"](#).
 - When the Threat Isolation Gateway functions as a Web Application Isolation Gateway, the Threat Isolation Engine (TIE), rather than the Threat Isolation Proxy, is responsible for end-user authentication.
-

4.7.12 Defining Gateway Clusters

4.7.12.1 Overview

When a Threat Isolation Gateway is created or updated, it is added to a Gateway cluster. A Gateway cluster defines a set of Gateways that are associated together within a Zone. Since clusters guarantee the availability of multiple Gateways at any given time, they ensure redundancy, a precondition for achieving load balancing. High availability and load balancing can be maintained with even a single cluster (for more information, see section [5 "High Availability and Load Balancing"](#).) Clusters also enable failover by preventing a single point of failure (SPOF).

Defining multiple clusters can be useful in the following scenarios:

- Grouping by geolocation – In large organizations, it can be efficient to group networks by their geographical location to make sure end users communicate with a Threat Isolation Engine (TIE) in their own region and not with a distant one. This can be done by defining multiple Gateway clusters, where the clusters share the same policy. Clusters also ensure that high availability and load balancing can be maintained within a specific geographical region.
- Migrating to a new Gateway version – A gradual and controlled transition to a new Gateway version can be facilitated by separating the production version from the new staging machines. Only Gateways in specific clusters will be upgraded, while Gateways in other clusters will stay with the previous version. You then route your users within the network to connect to Gateways in the relevant cluster.

Note

Adding the Report server and the Management Gateway to a cluster, which is mandatory, does not affect how these Gateways operate within the system.



4.7.12.2 Defining a Gateway Cluster

1. To create a Gateway Cluster object, go to:
System Configuration → Gateway Clusters → New Gateway Cluster
2. Configure the parameters described in the table below for the new Gateway Cluster object, and then click Create.

Column	Description	For More Information
General		
Name	Cluster name	
Description	Cluster description	
Timezone	Time zone of all Gateways belonging to this cluster	

Note

You cannot add Gateways to the new cluster from this object. You can assign Gateways to the Gateway cluster from the Gateways page when you create or update a Gateway (for more information, see sections [4.7.5 "Understanding the Gateway Settings Table"](#) and [4.7.7 "Defining a Threat Isolation Gateway"](#)). Once a Gateway has been assigned to a cluster, the Gateway Cluster page will display the name and description of the Gateway Cluster object and the Gateways associated with it.

4.7.13 Viewing Gateway Audit Logs

Audit log records are maintained on all cli-related events on Threat Isolation Gateway machines. The audit logs can be forwarded by means of log forwarding (see section [6.4 "Log Forwarding"](#)).

Note

Gateways audit log functionality requires a Report Server to be defined. See section [6.3 "Defining a Report Server"](#), and section [3.5.7 "Defining the Management Gateway"](#), Step 12, for enabling the Report Server.

Prerequisite

1. Go to:
System Configuration → Advanced Configuration
2. Search for auditing.gateways.show and make sure its value is true (default is false).
3. Refresh the browser.




To view the Gateways Audit Log

- Go to:

Management → Gateways Audit Log

The following table describes the Gateways Audit Log parameters.

Column	Description	For More Information
# (Number)	A number assigned to each log item	
Timestamp	The date and time of the event	
Action	<p>The action that occurred to trigger the log event</p> <p>An action is one of the following:</p> <ul style="list-style-type: none">■ SSH Session Created■ SSH Session Closed■ Password Change■ Authentication Failed■ Authentication Successful■ Terminal Command	
Gateway	The Gateway object name	
User	The user that has logged on to the Gateway machine and initiated the log event	
Command	<p>The command that was run</p> <p>Relevant only for Terminal Command</p>	
Return Code	<p>The message code returned by the OS after running the command: 0 on success; another value on failure (in this case, the OS returns the exit code).</p> <p>Relevant only for Terminal Command</p>	

- To refresh the Gateways Audit Log, click the  icon at the top right of the screen.
- For a detailed description of an audit log, click the line number or timestamp. Additional information is displayed by double-clicking the log record in the grid.



4.7.14 Integrating with Active Directory

1. Configure the system's use of Active Directory (AD). For information about defining AD settings, see section [4.5.2 "Defining Active Directory Settings"](#).
2. Associate AD with a Threat Isolation Proxy when defining a Threat Isolation Gateway. For information about defining and configuring a Threat Isolation Gateway, see section [4.7.7 "Defining a Threat Isolation Gateway"](#).

4.8 Configuring System Certificates

Define both types of system certificates that the Threat Isolation Gateway uses for a secure connection between the browser and the Gateway: CA certificates and server certificates.

4.8.1 System CA Certificates

A CA certificate is issued by a Certificate Authority (CA) and can sign new certificates in its name. When a CA certificate is trusted, all certificates below it in the hierarchy that were signed on its behalf will also be trusted.

The default CA certificate that Symantec Threat Isolation supplies out of the box is a self-signed certificate, meaning that it is signed by its own private key instead of by another Certificate Authority. For this reason, no browser will trust its issued certificates out of the box. If your organization wants to use the Symantec Threat Isolation Platform CA as a root CA, you must import the certificate and install it on the endpoint browser as a trusted root CA (see section [3.5.11.2 "Installing the CA Certificate in Windows Browsers"](#)), or deploy it through GPO (see section [3.5.11.1 "Deploying the CA Certificate File to the End Users"](#)).

Symantec Threat Isolation uses a CA certificate in the Zone for two purposes:

- Signing server certificates for the Threat Isolation Gateway, and
- Signing website certificates when the Gateway performs SSL termination (see section [3.5.7 "Defining the Management Gateway"](#)).



Note that Symantec Threat Isolation perform SSL termination only when Symantec Threat Isolation is operated in the topologies Symantec Threat Isolation Explicit Proxy (see section [2.6.2 "Symantec Threat Isolation Explicit Proxy"](#)) and Symantec Threat Isolation integrated with a third-party proxy (see section [Symantec Threat Isolation with Downstream Proxy Forwarding](#)). Only in these two modes does the Symantec Threat Isolation CA certificate sign server certificates. In the Symantec Threat Isolation as a Web Application Isolation Gateway Mode topology (see section [Symantec Threat Isolation as Web Application Isolation Gateway Mode](#)), Symantec Threat Isolation does not perform SSL termination and therefore does not need to sign certificates.

Symantec Threat Isolation allows you to define the CA certificate as an object that contains both the CA certificate and its private key. Since all Threat Isolation Gateways share the same Zone, you can define a CA Certificate object in the Zone, and then set up each individual Gateway to use the auto-generated server certificate signed by the Zone CA (see section [4.7.7 "Defining a Threat Isolation Gateway"](#)).

4.8.2 System Server Certificates

Symantec Threat Isolation uses a WebSocket to guarantee that the network protocol between the browser and the Threat Isolation Gateway is always secure. To enable a secure WebSocket to be established, a server certificate must reside on the Gateway.

Symantec Threat Isolation allows you to define server certificate objects that contain both the server certificate and its private key. The same server certificate object can be reused when you are working with multiple Gateways that share the same Public DNS name. These Gateways can share a single certificate, saving you from having to supply a key pair to each Gateway individually.

4.8.3 Adding a System Certificate

1. To add a system certificate, go to:

System Configuration → System Certificates → New System Certificate

2. Choose the relevant option:

- ◆ System CA Certificate, or
- ◆ System Server Certificate

3. Configure the parameters described in the table below for the new system certificate:



Parameter	Description	For More Information
General		
Name	Unique name you assign to this system certificate.	
Description	Description of the system certificate.	

4. Import the certificate key pair:

- ◆ Certificate - The certificate file.
- ◆ Private Key - The private key file that is paired with the certificate. This file can be encrypted (password protected) or not. In either case, the private key never resides in the Proxy machine's file system as clear text.

You can import each key as a file with a .pem extension, or provide it as text. The text option enables you to copy the certificate text (for example, from an e-mail) and paste it into the text editor. Symantec Threat Isolation validates the text and rejects it if it is incorrect.

5. If you provided the certificate as text, click Import to import the certificate.

4.9 Configuring Trusted Certificates

In certain scenarios, Symantec Threat Isolation must trust third-party certificates. Trusted certificates can be CA certificates and server certificates (for more information, see the sections [4.9.1 "Trusted CA Certificates"](#) and [4.9.2 "Trusted Server Certificates"](#)).

The Threat Isolation Gateway includes a set of out-of-the box CA certificates that the Symantec Threat Isolation Platform trusts. These certificates cannot be edited. You have the option of importing additional certificates (for more information, see section [4.9.4 "Trusting Only Imported Certificates"](#)).

4.9.1 Trusted CA Certificates

If your network topology includes a next hop proxy/server that performs SSL termination, the CA certificate of this next hop proxy/server will sign website server certificates. The endpoint browser needs to trust only the Threat Isolation Gateway. However, Symantec Threat Isolation is aware of the next hop proxy/server and must trust it. You must therefore add the CA certificate of the next hop proxy/server to the list of Symantec Threat Isolation trusted certificates.

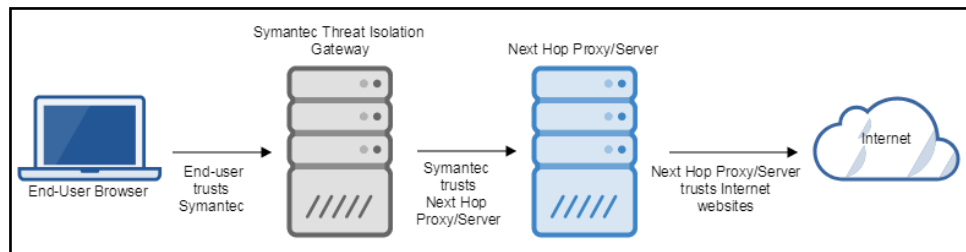


Figure 13 Trusted CA Certificate

If your organization uses a next hop proxy/server and your endpoints already trust its CA certificate, the Gateway can use the same certificate for simplicity's sake. In this case, you can import your next hop proxy/server's CA certificate into Symantec Threat Isolation (see sections [4.8.3 "Adding a System Certificate"](#) and [4.7.2 "Configuring the Zone"](#)). This CA certificate must be added both as a system certificate and as a trusted certificate.

Note

Symantec Threat Isolation system certificates contain both the certificate file and the private key. Trusted certificates contain only the certificate file.

4.9.2 Trusted Server Certificates

If your network topology does not include a next hop proxy/server, or if it includes a next hop proxy/server that does not perform SSL termination, the Threat Isolation Gateway might want to trust a server certificate. In this case, you need to import the trusted server certificate and add it to the list of Symantec Threat Isolation trusted certificates.

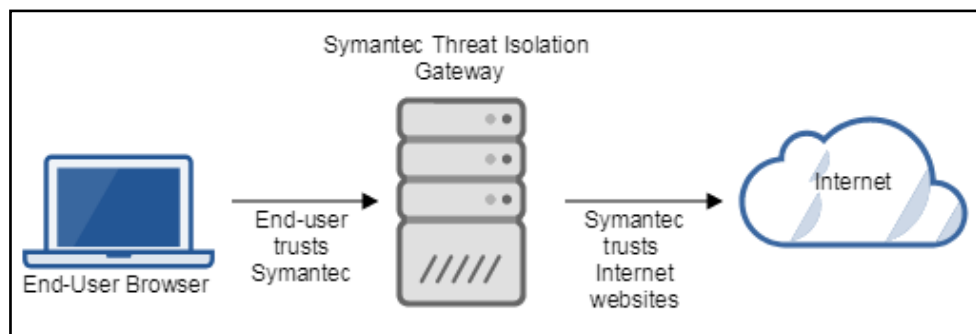


Figure 14 Trusted Server Certificate

Sometimes the Gateway needs to trust LAN resources, such as an Active Directory server that uses SSL for Active Directory connections (see section [4.5.2 "Defining Active Directory Settings"](#)) and has a server certificate that is signed by an



enterprise CA that is not trusted. In this case, the Gateway must trust the Active Directory server.

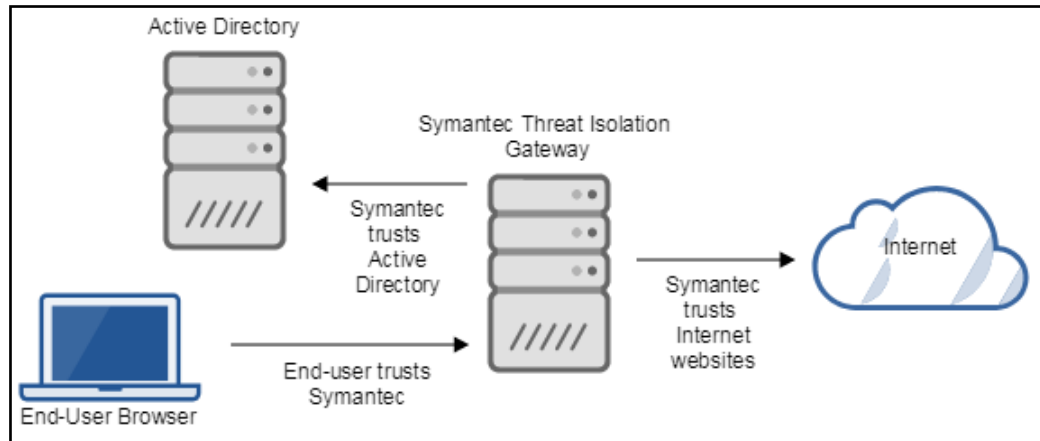


Figure 15 Trusted Active Directory

4.9.3 Adding a Trusted Certificate

- To add a trusted certificate, go to:
System Configuration → Trusted Certificates → New Trusted Certificate
- Choose the relevant option:
 - ◆ Trusted CA Certificate, or
 - ◆ Trusted Server Certificate – Currently, Symantec Threat Isolation supports trusted server certificates only in Isolation mode. If you require a trusted certificate in Inspect mode, provide a CA certificate instead.
- Configure the parameters described in the table below for the new trusted certificate:

Parameter	Description	For More Information
General		
Name	Unique name you assign to this trusted certificate	
Description	Description of the trusted certificate	
Trust		
Gateways	The Threat Isolation Gateway(s) that will trust this certificate	



4. Import the certificate file.

You can import the key as a file with a .pem extension, or provide it as text. The text option enables you to copy the certificate text (for example, from an e-mail) and paste it into the text editor. Symantec Threat Isolation validates the text and rejects it if it is incorrect.

5. If you provided the certificate as text, click Import to import the certificate.

4.9.4 Trusting Only Imported Certificates

Your organization might want to trust only CA/server certificates that were imported, and not those that Symantec Threat Isolation provides out of the box.

1. To trust only imported certificates, go to:

Gateway Advanced Settings > Internal Settings

2. Select the parameter `security_settings.trust_only_manual_certificate`.

For more information, see section [4.7.8 "Defining Gateway Advanced Settings"](#).

4.9.5 Adding Customized Text to the Untrusted Certificate Message

When the end user tries to visit a website with a server certificate that the Threat Isolation Engine (TIE) does not trust (i.e., the server certificate is not an out-of-the box CA certificate or a certificate you have imported), the following message is displayed in the endpoint browser: "Your connection is not private". You can add customized text (in red) to this message.

1. To add customized text to the untrusted certificate message, go to:

Policy Advanced Settings > Internal Settings

2. Edit the parameter `certificate_error_page_additional_text`.

For more information, see section [4.4.11 "Creating Policy Advanced Settings"](#).

4.10 Integrating a Downstream Proxy

When a third-party proxy is located between the endpoint and the Threat Isolation Gateway, that proxy must be integrated with Symantec Threat Isolation.

To integrate a downstream proxy:

1. Create a Downstream Proxy Settings object (see section [4.10.1 "Creating New Downstream Proxy Settings"](#)).
2. Click Push Settings to push the downstream proxy settings to the gateways. For more information, see section [4.7.6 "Pushing Settings"](#).



3. Do one of the following:
 - ◆ If you are using the Symantec Secure Web Gateway (ProxySG) as your downstream proxy, the Symantec Threat Isolation Platform provides dynamic instructions that enable you to configure and integrate the proxy semi-automatically (see section [4.10.2 "Configuring the Symantec Secure Web Gateway \(ProxySG\)"](#)).
 - ◆ If you are using any other product as your downstream proxy, contact Symantec Threat Isolation technical support to assist you with the proxy integration.

4.10.1 Creating New Downstream Proxy Settings

A third-party proxy, located between the endpoint and the Threat Isolation Gateway, must be defined in the Downstream Proxy Settings.

1. To create a Downstream Proxy Settings object, go to:
`System Configuration → Downstream Proxy Settings → New Downstream Proxy Settings`
2. Configure the parameters described in the table below for the new Downstream Proxy Settings object, and then click Create.

Column	Description	For More Information
General		
Product	<ul style="list-style-type: none">■ Symantec Secure Web Gateway (ProxySG)■ Other <p>NOTE: When ProxySG is used, configuration can be performed semi-automatically by running scripts that Symantec Threat Isolation generates, allowing for a smooth integration process. This convenience is not available when any other product is used.</p>	
Downstream Proxy Forwarding Settings		
Isolation Gateway Clusters	<p>The Gateway cluster(s) to which this downstream proxy forwards traffic.</p> <p>NOTE: A selected cluster must include at least one proxy and at least one Threat Isolation Engine (TIE). If it contains no Gateways, or only a proxy, or only TIEs, the selection will be considered illegal and an error message will be displayed</p>	



Column	Description	For More Information
Request Headers	<p>This downstream proxy adds designated request headers - Select when relevant</p> <p>Trust headers from IP(s) - Select the source IP address (es) of the downstream proxy. In case of multiple IPs, the addresses must be separated by a semi-colon (;). The Gateway will trust request headers only when they are sent from the specified IP address(es).</p> <p>Select the relevant designated request headers that this downstream proxy will add.</p> <p>For policy enforcement, the Threat Isolation Gateway will consider the value of these headers to be the source IP and username, respectively:</p> <ul style="list-style-type: none">■ X-Forward-For (XFF) Header■ X-Authenticated-User (XAU) Header. When selected, the Gateway does not need to authenticate the user. This setting determines whether the “Obtain user identity via X-Authenticated-User header” checkbox in the policy appears selected or clear. <p>NOTE: The activity log will only report the username that appears in the XAU header if a specific Access Role or “All authenticated users” has been specified in the matched rule’s User field. If the User field is empty, the activity log will report “Unauthenticated”.</p> <p>Request Headers - Whether to encode the XAU value to Base64 format.</p> <p>Header Format - Specify the format of the X-Authenticated-User value. Valid values:</p> <ul style="list-style-type: none">◆ “ (Supporting RFC): (\$scheme):/(\$domain)/(\$user)◆ “ (\$domain)\(\$user) <p>Only if the downstream proxy also acts as next hop proxy, these headers will be forwarded to the next hop proxy:</p> <ul style="list-style-type: none">■ X-Forward-For (XFF) Header■ X-Authenticated-User (XAU) Header■ X-Authenticated-Group (XAG) Header	<p>See section 4.2.2 “Editing Your Policy”</p>



Column	Description	For More Information
HTTPS Interception	(Relevant only for ProxySG) Select if this downstream proxy intercepts HTTPS isolated traffic. When this box is selected, you can configure if the same keyring will be used for all HTTPS traffic. If a different keyring is used for isolation traffic, specify its name.	
HTTPS Validation	(Relevant only for ProxySG) Specify the name of the CA Certificate List (CCL) for server certificates that ProxySG uses. The default option is the browser-trusted CCL. The alternative option enables you to specify a different CCL name.	
Isolation Criteria	(Relevant only for ProxySG) Select to isolate only websites that meet specific criteria. When the box is selected, specify the conditions for isolation. Clear the checkbox to isolate all websites.	See section 4.10.1.1 "Isolation Criteria"
Next Hop Proxy Settings		



Column	Description	For More Information
Next Hop Proxy	<p>Select if this downstream proxy also serves as next hop proxy. When this box is selected, the corresponding Next Hop Proxy Settings will be updated automatically.</p> <p>You can view the settings for the corresponding Next Hop Proxy Settings object in the Next Hop Proxy Settings table. Note that you can create, update and delete the Next Hop Proxy Settings object, as well as edit some of its properties, only from the Downstream Proxy Settings object.</p> <p>Select if your next hop proxy is transparent or explicit. If explicit, provide its address and port:</p> <p>Address - URL address for the next hop proxy server. This is the address to which the Gateway connects</p> <p>Port - The specified access port to the next hop proxy server</p> <p>Next Hop CA - Add the CA certificate of the next hop proxy to the list of Symantec Threat Isolation trusted certificates</p> <p>Click Edit to display:</p> <p>Advanced Settings</p> <p>Customized User Header - If the next hop proxy expects a header other than the standard X-Authenticated-User (XAU) header, specify the customized header</p> <p>Customized Groups Header - If the next hop proxy expects a header other than the standard X-Authenticated-Groups (XAG) header, specify the customized header</p> <p>Custom Threat Isolation Username - Select to add a custom user name for outgoing requests initiated by the Threat Isolation Gateway. Specify the custom username below</p> <p>Custom Threat Isolation Header - Select to add a custom header for outgoing requests initiated by the Threat Isolation Gateway. Specify the custom header name below</p>	<ul style="list-style-type: none">■ See section 3.6.2 "Configuring Symantec Threat Isolation with Downstream Proxy Forwarding",■ See section 4.11 "Creating New Next Hop Proxy/Server Settings", 4.11 "Creating New Next Hop Proxy/Server Settings"
Cluster Diagnostics		



Column	Description	For More Information
	The table lists the association between clusters and related Gateway (s). If at least one cluster contains an error, an error message will be displayed	
Instructions		
	Dynamic instructions per environment for automatic downstream proxy configuration.	

For more information, see section [3.6.2 "Configuring Symantec Threat Isolation with Downstream Proxy Forwarding"](#).

4.10.1.1 Isolation Criteria

This section is relevant only when Symantec Secure Web Gateway (ProxySG) is your downstream proxy.

The criteria for website isolation must be provided as a Content Policy Language (CPL) condition. For more information about CPL, see https://support.symantec.com/en_US/article.DOC10455.html.

For your convenience, Symantec Threat Isolation provides a basic CPL condition that you can change according to your organization's needs by editing, adding to, and uncommenting the relevant lines. Note that the syntax used in this condition is relevant to the ProxySG Web Access layer.

The following default condition is provided:

```
define condition Threat_Isolation_CondWebIsolationMatchCriteria
    ;url.threat_risk.level=7..10
    ;url.category=("Malicious Outbound Data/Botnets","Suspicious")
    ;url.domain="malicious.com"
    ;authenticated=yes
    ;client.address=192.168.10.0/24
    ;authenticated=yes url.category=("Malicious Outbound
Data/Botnets")
end condition Threat_Isolation_CondWebIsolationMatchCriteria
```

Guidelines

To isolate risky websites, uncomment the following line:

```
;url.threat_risk.level=7..10
```



To isolate risky websites OR specific categories, uncomment both of the following lines:

```
;url.threat_risk.level=7..10  
  
;url.category=("Malicious Outbound Data/Botnets", "Suspicious")
```

To isolate authenticated users AND specific categories, uncomment the following line:

```
;authenticated=yes url.category=("Malicious Outbound  
Data/Botnets")
```

Note that OR logic is defined by two or more lines, while AND logic is defined by two gestures within the same line.

You can continue to edit or add to the relevant lines per your requirements.

4.10.2 Configuring the Symantec Secure Web Gateway (ProxySG)

If you are using the Symantec Secure Web Gateway (ProxySG) as your downstream proxy, the Symantec Threat Isolation Platform provides dynamic instructions that enable you to configure and integrate the proxy semi-automatically. These convenient dynamic instructions are not available for products by any other vendor.

Part of the ProxySG configuration can be done using a script with command line interface commands that you can copy and paste into the ProxySG appliance CLI. Another part can be done using Content Policy Language (CPL).

To perform the ProxySG configuration semi-automatically, follow the instructions in the ProxySG Automatic Configuration window:

1. Activate command privileged mode by running the relevant ProxySG commands.
2. Configure the ProxySG using Command Line Interface (CLI) commands.

You can run the ProxySG commands interactively, or use a script.

When using a script, download the script or copy it by using the appropriate button, then paste its contents after the prompt in command privileged mode.

3. To reflect the outcome of the CLI configuration change in the ProxySG Management Console, close and open the browser.



4. Configure the ProxySG using Content Policy Language (CPL).

The CPL content in this section refers to the ProxySG Visual Policy Manager configuration.

- ◆ For VPM users - In the ProxySG Visual Policy Manager, add a CPL layer (suggested name: Isolation CPL Layer). **Important:** This CPL layer must be the final layer. Download or copy the CPL content and paste it into the new layer.
- ◆ For non-VPM users - **Important:** The content must be appended to the final installed file: Local/Forward/Central.

5. Click Install Policy.

4.11 Creating New Next Hop Proxy/Server Settings

When a next hop proxy/server is located between the Threat Isolation Gateway and the Internet, that proxy must be defined in Next Hop Proxy/Server Settings. Once the next hop proxy/server is set up, the Gateway is instructed to reach the Internet via this next hop proxy/server.

1. To create a Next Hop Proxy/Server Setting object, go to:

System Configuration → Next Hop Proxy/Server Settings
→ New Next Hop Proxy/Server Setting

2. Configure the parameters described in the table below for the new Next Hop Proxy/Server Setting object, and then click Create.

Column	Description	For More Information
General		
Select whether your next hop proxy/server is transparent or explicit. If it is explicit, provide its address and port		
Mode	Select whether your next hop proxy/server is transparent or explicit. Only if it is explicit, provide its address and port:	
Address	URL address for the next hop proxy/server	
Port	The specified access port to the next hop proxy/server	
HTTPS Interception	Select when this next hop proxy/server intercepts HTTPS	
Modifying HTTP(S) Traffic		



Column	Description	For More Information
Request Headers	<p>The Threat Isolation Proxy will:</p> <ul style="list-style-type: none">■ Add the X-Forwarded-For header, containing the originating IP address for which the request was forwarded, to outgoing requests■ Add the X-Authenticated-User header, containing the authenticated username, to outgoing requests. <p>NOTE: When one or more of the above headers are selected, the Gateway assumes that the next hop proxy/server is responsible for removing the header from the request before forwarding it to the Internet</p>	<ul style="list-style-type: none">■ See section 4.11.1 "X-Forwarded-For (XFF) Request Header"■ See section 4.11.2 "X-Authenticated-User (XAU) Request Header"
Advanced		
Exceptions	<p>A list of hostnames or IP addresses that are not routed through this next hop proxy/server</p> <p>Each hostname or IP address must be separated by a semicolon (;)</p> <p>Wildcards (*) can be used for hostnames. For example, *.cnn.com</p>	
Customized User Header	<p>If the next hop proxy/server expects a header other than the standard X-Authenticated-User (XAU) header, specify the customized header</p>	
Encode User Header	<p>Whether to encode the XAU value to Base64 format</p>	
Header Format	<p>Specify the format of the X-Authenticated-User value. Valid values:</p> <ul style="list-style-type: none">■ Default (supporting RFC): (\$scheme):/(\$domain)/(\$user)■ Use (\$scheme), (\$domain) and (\$user). Any combination of these variables is valid	
Add Threat Isolation Username	<p>Whether to add a customized user name for outgoing requests initiated from the Threat Isolation Gateway</p>	
Add Threat Isolation Header	<p>Whether to add a customized header for outgoing requests initiated from the Threat Isolation Gateway</p>	

**Note**

This next hop proxy/server setting must be associated with the Threat Isolation Gateway to take effect. For more information, see sections [4.7.7 "Defining a Threat Isolation Gateway"](#) and [4.7.7.1 "Configuring a Next Hop Proxy/Server"](#).

4.11.1 X-Forwarded-For (XFF) Request Header

The Threat Isolation Gateway adds the X-Forwarded-For (XFF) header, which contains the originating IP address for which the request was forwarded, to the outgoing request. The next hop proxy/server removes the XFF header from the request before forwarding it to the Internet.

4.11.2 X-Authenticated-User (XAU) Request Header

The Threat Isolation Gateway adds the X-Authenticated-User (XAU) header, which contains the authenticated username, to the outgoing request. The next hop proxy/server removes the XAU header from the request before forwarding it to the Internet.

4.12 Configuring Email Servers

Depending on your system topology, you might have to add a new email server. Email servers are used for monitoring alerts. When an alert is fired, it can also be sent to an email via an email server in the network.

1. To define a new email server, go to:
System Configuration → Email Servers → New Email Server
2. Configure the parameters described in the following table for the new email server, and then click Create.

Parameter	Description	Additional Information
General		
Active	Select to use this server Important: Even when this email server is referenced by other entities, this checkbox determines whether or not it will be used	
Connection		
Host	External mail server host	



Parameter	Description	Additional Information
Port	Port through which the email server communicates	<ul style="list-style-type: none">■ The port is configurable. Default: 465■ Connectivity from the Management server to this server is accessed via this port
Security	Select to use TLS to secure communication	
Authentication		
Authenticate with Email server	Select if the email server requires authentication	
Username	Username used for authentication with the email server	
Password	Username's password used for authentication with the email server	
Email Message		
From	Email address from which the email originated	
To	Email address to which the email is sent	

4.13 Configuring SNMP Servers

Threat Isolation Gateways send system metrics, such as disk status, CPU status, and so on, as well as application metrics to the Management server using the metrics threshold mechanism (see section [7.3 "Metric Thresholds"](#)).

The Management server collects these metrics, and when a metrics threshold is crossed, it sends both system metrics and application metrics to the SNMP server via SNMP traps. The standard Linux MIB is exposed; the top level of the MIB's OID is .1.3.6.1.2.1.1. For this purpose, the SNMP server must be set up with a Monitor Group. For more information, see section [7.2 "Monitor Groups"](#).

The following logs will be forwarded to SNMP servers: Event logs.

**Note**

- The Management server sends both system metrics and application metrics for which the metrics threshold was crossed to the SNMP server via SNMP traps.
- The Gateway exposes only system metrics on demand, in response to SNMP Walk/GET requests by the SNMP server (see the field “Expose system metrics” in section [4.7.7 "Defining a Threat Isolation Gateway"](#)).

1. To define a new SNMP server, go to:
System Configuration → SNMP Servers → New SNMP Server
2. Configure the parameters described in the following table for the new SNMP server, and then click Create.

Parameter	Description	Additional Information
General		
Active	Defines whether or not the Management server can send traps (alert messages) to this SNMP server Important: Even when this SNMP server is referenced by other entities, this checkbox determines whether it will be sent traps	
MIB File	The Management Information Base (MIB) file stores customized system Object Identifiers (OIDs). Download this file and import it into the SNMP server	See section 7.3 "Metric Thresholds" . All thresholds in this section are mapped in the MIB file
Connection		
Host	SNMP server host name or IP address	
Port	Port through which this server communicates	Default port for sending traps to the SNMP server: 162



Parameter	Description	Additional Information
Community Name	<p>String used to authenticate SNMP requests. Default: "public"</p> <p>NOTE: The community name configured here is not the same as the one configured in the Gateway object:</p> <ul style="list-style-type: none">■ The community name configured here is used by the Management Server to authenticate to the new SNMP server that you are defining.■ The community name configured in the Gateway object is used by an external SNMP server to authenticate to the Gateway to send it SNMP requests.	

Note

The SNMP server must be set up with a Monitor Group to become operational. For more information, see section [7.2 "Monitor Groups"](#).

4.14 Configuring Syslog Servers

Depending on your deployment topology, you might need to define a system log (Syslog) server.

The following logs will be forwarded to the syslog server: Event logs, Management audit logs, Gateway audit logs, and activity logs.

1. To define a new syslog server, go to:

System Configuration → External Log Server → New External Log Server → Syslog Server

2. Configure the parameters described in the following table for the new syslog server, and then click Create.

Parameter	Description	Additional Information
General		
Active	<p>Select to use this server</p> <p>Important: Even when this syslog server is referenced by other entities, this checkbox determines whether or not it will be used</p>	
Connection		
Host	Syslog server host name	IP Address or FQDN



Parameter	Description	Additional Information
Port	Port through which this server communicates	<ul style="list-style-type: none">■ The port is configurable. Default: 514■ Connectivity from the Management server to this server is accessed via this port
Protocol	Protocol this server uses for communication	<ul style="list-style-type: none">■ The protocol is configurable. Default: UDP
Appname	Tag used to identify Symantec Threat Isolation application	
Facility	Syslog facility name related to Symantec Threat Isolation logs	

Note

The syslog server must be set up with log forwarding to become operational. For the log forwarding setup, see section [6.4 "Log Forwarding"](#).

4.15 Configuring ArcSight Servers

Depending on your deployment topology, you might need to define an ArcSight server. The common event format is utilized within the ArcSight protocol requirements. The following logs will be forwarded to the ArcSight server: Activity logs.

1. To define a new ArcSight server, go to:

System Configuration → ArcSight Configuration → New ArcSight Server

2. Configure the parameters described in the following table for the new ArcSight server, and then click Create.

Parameter	Description	Additional Information
General		
Active	Select to use this server Important: Even when this ArcSight server is referenced by other entities, this checkbox determines whether or not it will be used	
Connection		



Parameter	Description	Additional Information
Protocol	Protocol this server uses for communication. Options include UDP, TCP or AWS S3	<ul style="list-style-type: none">■ The protocol is configurable. Default: UDP■ See section 4.15.1 "AWS S3 Protocol Configuration" for AWS S3 protocol configuration
Host	ArcSight server host name	IP Address or FQDN
Port	Port through which this server communicates	<ul style="list-style-type: none">■ The port is configurable. Default: 514■ Connectivity from the Management server to this server is accessed via this port

Note

The ArcSight server must be set up with log forwarding to become operational. For the log forwarding setup, see section [6.4.1 "Configuring Log Forwarding"](#).

4.15.1 AWS S3 Protocol Configuration

The AWS S3 protocol offers the ability to save ArcSight log files to the Amazon cloud. This requires your own AWS account, additional firewall settings and access from the report server machine (see section [6.3 "Defining a Report Server"](#) for information about defining a report server). The log files are transferred to the Amazon Cloud when either a certain amount of time has passed since the last file transfer, or a file size limit has been reached.

When selecting the AWS S3 protocol, you must configure the following parameters:

Parameter	Description	Additional Information
Time Rotation (in minutes)	The length of time before a file is transferred to the AWS	
Size Rotation (in Mbytes)	The file size before a file is transferred to the AWS	
AWS provides the following parameters with your configured account: <ul style="list-style-type: none">■ Bucket■ Directory■ Region■ Access Key ID■ Secret Access Key		

**Note**

Both time and size are verified before a file is transferred. When either condition is met, the file is rotated to the AWS.

4.15.2 ArcSight CEF Mapping

To facilitate a common format between Symantec Threat Isolation and your Security Information and Event Management (SIEM) system, data fields must be mapped.

Below is a list of common event format (CEF) fields that map Symantec Threat Isolation fields to the CEF fields. The event is set by the Symantec Threat Isolation activity log events; severity is always set to a value of 6 in a range of 1-10, with 10 being the most severe event. Common SIEM systems that support this mapping include ArcSight and Graylog. For an example of CEF content, see section [4.15.2.1 "Sample CEF Content"](#).

The table below describes the required CEF fields mapping.

CEF header field	Internal field in Activity Log JSON data ^[1]	Description	Sample value
Device Event Class ID	event	Unique identifier per event type. Contains the name of the event.	Network Request
Device Product	-	String that identifies the device producing the data.	Threat Isolation (constant)
Device Vendor	-		Symantec (constant)
Device Version	-		1.0 (constant)
Name	event	String representing a human-readable and understandable description of the event.	Network Request
Severity	-	Integer that reflects the severity of the event in the range 1-10, with 10 being the most severe.	6 (constant)
Version	-	Integer that identifies the version of the CEF format. The current CEF version is 0.	CEF:0 (constant)

^[1] For information about internal fields in the activity log, see section [6.1.2.2 "Activity Log Event Window"](#).



The table below describes CEF extension fields mapping.

CEF field	Internal field in Activity Log JSON data ¹²	Description	Valid value	Sample value
act	action	Policy action for a requested URL	Isolate, Block, Pass, Inspect	Isolate
app	url_scheme	Requested URL scheme	about, blob, chrome-devtools, data, ftp, http, https	https
cat	event	Unique identifier per event type. Contains the name of the event	Forward To Isolation, Network Request, Session Ended, Print, Isolation Suspension Request, Tab Closed, Clipboard Copy, Clipboard Copy Blocked, Clipboard Paste Blocked, Clipboard Paste, File Download, File Upload, Flash Loaded, Keyboard, Mouse, Phishing, Drive-By Download, Read-Only Page, Input Authentication Request, Redirect To Proxy, End-User Experience	Isolation Suspension Request



CEF field	Internal field in Activity Log JSON data ¹²	Description	Valid value	Sample value
dhost	url_host	The host name of the request URL	Valid host	z.cdn.cnn.com
dlat	latitude	Geolocation latitude	Number	54.0
dlong	longitude	Geolocation longitude	Number	-2.0
dpt	url_port	HTTP request destination port	Positive number	443
dst	destination_ip	Destination IP address for the request	IPv4, IPv6	82.166.201.169
dvchost	host	Web Isolation Gateway that originated the log entry	Gateway object name	gw1
externalId	log_unique_id	Log record uuid	GUID	fcabc2792-a604-40e0-833f-9a3c9cf364ec
fileHash	md5	MD5 hash (or checksum) of a file	String	79054025255fb1a26e4bc422aef54eb4
fileId	mime_type	Media type of the downloaded/uploaded file	Valid mime-type	application/zip
filePath	file_path	The path in the Gateway from where the file was uploaded		
fileType	file_type	Extension of the downloaded/uploaded file	Valid file extension	zip
fname	file_name	Name of the downloaded/uploaded file	String	Presentation.zip



CEF field	Internal field in Activity Log JSON data ¹²	Description	Valid value	Sample value
fsize	total_bytes (for downloaded file) total_bytes_sent (for uploaded file)	Size of the downloaded/uploaded file	Number	10485760
in	total_bytes_sent	The size of the sent traffic	Number	101
out	total_bytes	The size of the received traffic	Number	43
outcome	content_action	Policy action for a requested file	Blocked, Allowed, Viewed, Scanned, Infected	Blocked
reason	details	Information about the log record. If the log record has a severity value, the details field will be populated with a reason.	String	
	description	Description of the isolation suspension request, given by the end user		
request	url	Requested URL	URL	http://z.cdn.cnn.com/cnn/.e/fonts/3.1.0/fonts/cnnsans-thinit.woff2



CEF field	Internal field in Activity Log JSON data ¹²	Description	Valid value	Sample value
requestClientApplication	user_agent	HTTP request header: User-Agent	String	Mozilla/5.0 (Windows NT 10.0; WOW64; Trident /7.0; Touch; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; Tablet PC 2.0; rv:11.0) like Gecko
requestContext	referrer_url	The URL that referred the current request	URL	http://edition.cnn.com/election/results/?****
requestMethod	request_method	HTTP request method	CONNECT, DELETE, GET, HEAD, OPTIONS, POST, PUT	
rt end start	@timestamp	The time (UTC) when the Gateway recorded the event.	UTC Format: MMM dd YYYY HH:mm:ss.SSS zzz	Nov 16 2016 15:20:55. 512 UTC
sntdom	username (parsed)	Source user domain name	String	bigcorp.local
sourceServiceName	service	The Web Isolation component that originated the log entry	Proxy, Threat Isolation Engine, Reverse Proxy	
sproc	client_name	Client-friendly name, parsed from the user agent	Chrome, Firefox, IE, Opera, Safari, Edge, Unidentified, Other	Chrome



CEF field	Internal field in Activity Log JSON data ¹²	Description	Valid value	Sample value
spt	source_port	Source IP of the endpoint/downstream proxy	Positive number	1234
src	source_ip	Source IP of the endpoint. The xff value is also populated here	IPv4, IPv6	192.168.56.1
suser	username (parsed)	Source username - alias only	String	graham.norton
SymantecThreatIsolationTenantId	tenant_id	Tenant ID	String	D4422-AODDA-A7ADE-FBF77-BD881

The table below describes CEF fields mapping - custom numbers.

CEF header field	Internal field in Activity Log JSON data ^[1]	Description	Valid value	Sample value
cn1	policy_version	Pushed settings version	Number	230
cn1Label	-	Label	String	Policy Version
cn2	response_status_code	HTTP response status code	Number	200
cn2Label	-	Label	String	Response Status Code
cn3	url_risk	Requested URL risk level	Number between 0 and 10 (0 means risk categorization failure)	9
cn3Label	-	Label	String	URL Risk Level

[1] For information about internal fields in the activity log, see section [6.1.2.2 "Activity Log Event Window"](#).



The table below describes CEF fields mapping - custom strings.

CEF header field	Internal field in Activity Log JSON data ^[1]	Description	Valid value	Sample value
cs1	rule_id	The ID of the rule that was matched when the event happened	Number	3
cs1Label	-	Label	Rule ID	Matched Rule ID
cs2	session_id	Unique Session ID (only for TIE logs), changes upon browser refresh and browser address bar change	GUID	a835a98db563a4c8_93573_3
cs2Label	-	Label	Session ID	Isolation Unique Session ID
c3	action_reason	The reason for the policy action	Polyc Rule, Subresource, Fail Open, Invalid Url	Invalid Url
cs3Label	-	Label	String	Action Reason
cs4	url_categories	Requested URL categories	Array of categories	
cs4Label	-	Label	Parent URL Categories	Technology/Internet
cs5	rule_name_at_log_time:rule_type	The name of the rule that was matched when the event happened followed by its type	String:string	Default Rule:default
cs5Label	-	Label	Rule Name (At Log Time)	Matched Rule Name (At Log Time)
cs6	top_level_url	The website URL as it appeared in the browser address bar when the event took place (relevant only for isolated websites)	URL	http://edition.cnn.com/
cs6Label	-	Label	URL	Website URL

^[1] For information about internal fields in the activity log, see section [6.1.2.2 "Activity Log Event Window"](#).



4.15.2.1 Sample CEF Content

In CEF content, required CEF fields are separated by | and ordered according to their order in the table. In the sample below, optional extension fields are shown in blue:

```
CEF:0|Symantec|Threat Isolation|1.0|Network Request|Network  
Request|6|rt=Jun 03 2018 12:40:48.123 UTC end=Jun 03 2018  
12:40:48.123 UTC start=Jun 03 2018 12:40:48.123 UTC  
externalId=fcbc2792-a604-40e0-833f-9a3c9cf364ec cat=Network  
Request sproc=Chrome sourceServiceName=Threat Isolation Engine  
request= https://usermatch.krxd.net/um/v2?partner=vdna  
requestMethod=GET requestContext= src=10.0.80.80 spt=  
dst=80.249.99.148 dhost= usermatch.krxd.net dlat=54.0 dlong=-2.0  
dpt=80 requestClientApplication=Mozilla/5.0 (Windows NT 6.1;  
Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)  
Chrome/66.0.3359.181 Safari/537.36 fname= filePath= fileType=  
fileHash= fileId= fsize= suser=Unauthenticated sntdom= app=http  
in=0 out=5242880 act=Isolate dvchost=fireglass1 reason= outcome=  
cn1=70 cn1Label=Policy Version cn2=200 cn2Label=Response Status  
Code cn3=0 cn3Label=URL Risk Level cs1=1 cs1Label=Matched Rule ID  
cs2=a42070ac1bb18de7_17641_6 cs2Label=Isolation Unique Session ID  
cs3=Policy Rule cs3Label=Action Reason cs4=Technology/Internet  
cs4Label=URL Categories cs5=Default Rule:default cs5Label=Rule  
Name (At Log Time) cs6= http://www.bbc.com/earth/world  
cs6Label=Website URL SymantecThreatIsolationTenantId=
```

4.16 Configuring Apache Kafka Servers

Depending on your deployment topology, you might be able to forward logs to a Kafka server. The following logs will be forwarded to the Kafka server: Activity logs.

1. To define a new Kafka server, go to:

System Configuration → External Log Servers → New External Log Server → Kafka Server

2. Configure the parameters described in the following table for the new Kafka server, and then click Create.

Parameter	Description	Additional Information
General		
Name	Unique name assigned to this Kafka server	Required



Parameter	Description	Additional Information
Active	Select to use this server Important: Even when this Apache Kafka server is referenced by other entities, this checkbox determines whether or not it will be used	
Connection		
Hosts	List of hosts and ports to be used for connecting to the Kafka cluster	Required Must be a comma-separated list of hosts and ports, in this format: host:port The port is configurable. It can be specified after the colon, for example: server1.corp:2181, server2.corp:2181, and so on
Topic ID	The name of the topic under which the log items are sent	Required
Advanced		
Security Protocol	Select the required security protocol	Required Possible values: <ul style="list-style-type: none">■ Plaintext■ SSL
Compression Type	The type of compression to use when communicating with the Kafka server	Required
Acknowledgments Needed	Acknowledgments needed to consider a message sent	Required Possible values: <ul style="list-style-type: none">■ None■ All Kafka members in the cluster■ Only the leader of the cluster



Parameter	Description	Additional Information
Batch Size (Bytes)	Messages are grouped and sent in batches. This setting sets the maximum batch size, in bytes	Optional. If not set, the default will be used (set by the underlying infrastructure) Possible values: <ul style="list-style-type: none">■ Minimum: 1 byte■ Maximum: 512 MB
Metadata Refresh Maximum Time (Milliseconds)	The period of time, in milliseconds, after which a metadata refresh is forced even if no partition leadership changes were seen to proactively discover new brokers or partitions	Optional. If not set, the default will be used (set by the underlying infrastructure) Possible values: <ul style="list-style-type: none">■ Minimum value: 1■ No maximum value

Notes

- The Kafka server must be set up with log forwarding to become operational. For the log forwarding setup, see section [6.4.1 "Configuring Log Forwarding"](#).
- The Kafka server must be able to receive communications from the Symantec Threat Isolation report server machine. Make sure this is allowed by the firewall settings on the Kafka machine.

4.17 Configuring Cynic Server Settings

The Symantec Threat Isolation Platform is integrated with a number of third-party tools that allow files to be sent to a sandbox for analysis. One such tool is Symantec Cynic™, a cloud-based sandboxing system.

To use Symantec Cynic, upload its license to Symantec Threat Isolation Management and enable Symantec Cynic in the Download Profile, under File Sanitizers (for more information, see section [4.3.4.4 "Adding a Download Profile"](#)). Symantec Cynic will then be used for scanning file types associated with this Download Profile.

1. To define new Cynic server settings, go to:
`System Configuration → Cynic Server Settings → New Cynic Server Setting`
2. Configure the parameters described in the following table for the new Cynic server, and then click Create.



Parameter	Description	Additional Information
General		
Scanning Mode	Select the default scanning mode: <ul style="list-style-type: none">■ Hold (default) - The file is submitted for inspection while the verdict is awaited■ Background - The file is submitted for inspection and downloading is allowed In both modes, when the same file is downloaded again in the future, Cynic will recognize the file and return a verdict immediately	See section 4.3.4.5 "Defining Download Profiles Advanced Settings"
Symantec License File	Select the Symantec Cynic license file	

4.18 Configuring Data Leakage Prevention Server Settings

Data Leakage Prevention Server Settings prevent sensitive data, such as credit card information and Social Security numbers, from being leaked to entities outside of the organization. Specified file types are prevented from being uploaded to a website if they conflict with the Data Leakage Prevention (DLP) policy.

When Symantec Threat Isolation is integrated with Symantec Data Loss Prevention¹, you are notified of DLP events. The specific DLP violation(s) will be provided in the notification. In addition, you can choose to have Symantec Threat Isolation notify the end user when a DLP event has occurred. Currently, Symantec Threat Isolation supports Symantec Data Loss Prevention's "Block Data-in-Motion" action.

The following must be configured in the Symantec Data Loss Prevention Enforce Server:

- Select "Match On: Attachments" to scan files
- Select "Match On: Body" to scan network requests

4.18.1 Adding Data Leakage Prevention Server Settings

1. To access the Data Leakage Prevention Server Settings page, go to:

System Configuration → Data Leakage Prevention Server Setting

¹For more information, see <https://www.symantec.com/products/data-loss-prevention>.



2. Add a new Data Leakage Prevention Server Setting by clicking New Data Leakage Prevention Server Setting.
3. Configure the parameters described in the table below for the new data leakage prevention server setting, and then click Create.

Parameter	Description	For More Information
Data Leak Prevention Settings		
Certificate File	Password-protected client certificate file, in PKC12 format. This certificate enables the Threat Isolation Gateway to prove that it is authorized to consume the Data Leakage Prevention (DLP) service	
Certificate Passphrase	The passphrase to be provided for the client certificate file	
Detector Id	The target detector ID of the DLP policy to be used. This ID is used for routing the detection request to the appropriate back-end service	See Note, below
Detector URL	The URL to which the Gateway will connect in order to consume the service	
Rest Connector GUID	Your Global Unique ID (GUID) as consumer of the service, used by the third party's server for policy targeting	

Note

For the Symantec™ Data Loss Prevention Cloud Service Connector REST API Reference Guide, follow the link:

https://support.symantec.com/en_US/article.DOC9417.html#403

4.19 Editing Advanced Configuration

Sometimes it might be necessary to view or edit the Symantec Threat Isolation Advanced Configuration Settings.

Note

Changing the Advanced Configuration Settings might result in unexpected system behavior, and should only be done in consultation with Symantec Threat Isolation technical support. Some changes require a service restart.

1. To edit the Advanced Configuration Settings, go to:
Advanced Configuration → Advanced Configuration Settings



Advanced Configuration Settings				
Warning: Changing the advanced settings may result in unexpected behaviour and should only be done in consultation with technical support. Some changes require a service restart.				
Search <input type="text"/>				
Name	Value	Description	Updated At	Actions
activityLogConfiguration.logAllQueryParams	false		6 months ago	
antivirus.isFailOpen	false		6 months ago	
antivirus.metaScanCloud.api.key	eeccad4e39ca5c293b8d03f9d8fb3a1		6 months ago	
antivirus.metaScanCloud.api.key	eeccad4e39ca5c293b8d03f9d8fb3a1		6 months ago	
antivirus.metaScanCloud.api.scanTimeout	60000		6 months ago	
antivirus.metaScanCloud.api.threshold	0.2		6 months ago	
antivirus.metaScanServer.api.maxRetries	10		6 months ago	

2. Using the Search bar, search for the parameter you want to update.
3. Under Actions, click the edit icon for the parameter and make the necessary changes.

4.20 Licensing

To be able to make full use of the Symantec Threat Isolation Platform, you must provide a license. For more information on the different offerings, consult with your Symantec sales representative.

4.20.1 Registering your Licensed Components

4.20.1.1 Prerequisites

In the components registration procedure, several steps must be performed in Symantec's Network Protection Licensing Portal (NPLP).

Display the NPLP as follows:

https://services.bluecoat.com/eservice_enu/licensing

In the NPLP, retrieve the VA Serial Number:

1. Select Isolation > VA Serial Number Retrieval from the left menu.
2. Specify the Activation Code that Symantec provided by email when the components were purchased, and then click Submit.

The Management VA Serial Number is returned. From this point forward, this serial number is the Symantec Identity for your device.

4.20.1.2 Registration

If you are an upgrading customer and have never registered your device, or if you have postponed registering when you defined the Management Gateway, using the First Time Wizard, you can register your licensed components as follows:



1. Go to:
System Configuration → Licensing → New License Settings
2. In the Create License Settings window, perform one of the following.
 - ◆ **Online registration**
 - i. Under Registration Information, select Online Registration.
 - ii. Provide the following:
 - Your MySymantec customer login credentials, which you specified when you created a MySymantec Account (as a Getting Started step described in the Fulfillment Acknowledgment email)
 - The VA Serial Number
 - iii. Click Register.
 - iv. Click Push Settings.
 - ◆ **Offline registration**

Prerequisite

From the NPLP, download the license file as follows:

 - i. i. Select Isolation > License Download from the left menu.
 - ii. Specify the VA Serial Number and a PassPhrase.

Note

The PassPhrase is used to encrypt the license file and must include at least eight alphabetic and/or numeric characters. It is required only when you register the licensed components for the first time.

- iii. Click Next, and then download the license file.

Registering Offline

In the Create License Settings window, do the following:

- i. Under Registration Information, select Offline Registration.
- ii. Click Register... and then choose the downloaded license file from your file system. The file has the following format: license_<serial_number>.bcl.
- iii. In the License File Passphrase pop-up window, type the PassPhrase you specified in the NPLP (see step ii., above).
- iv. Click OK.



- v. Click Push Settings.

4.20.1.3 Viewing Current License Information

Only when your licensed components have been registered, you can view current license information (activation date, expiration date and product description) for the licensed components in the License Settings window, under License Information. Note that currently, the status of add-ons is not reflected here. If you have activated add-ons, you can view their status in the Network Protection Licensing Portal (NPLP).

1. To view current license information, go to:
`System Configuration → Licensing`
2. Under Actions, click the edit icon in the row of the relevant license.

4.20.1.4 Updating a License

1. To update a license, go to:
`System Configuration → Licensing`
2. Under Actions, click the edit icon in the row of the relevant license.

The Update License Settings window allows you to view current license information and update your licenses.
3. Click Update, and then do one of the following, per your requirements:
 - ◆ Select Online to force a license update.
 - ◆ Select Offline... to update your license offline. The License Update File window appears.

Prerequisite

Go to the Network Protection Licensing Portal (NPLP) (https://services.bluecoat.com/eservice_enu/licensing) and do the following:

- i. From the left menu, select Isolation > License Download.
- ii. Specify the VA Serial Number, and then click Next. NOTE: There is no need to provide a PassPhrase here.
- iii. Download the license file.



Updating the License

In the License Update File window:

- i. Click Browse, and then browse to the license file that you have downloaded from the NPLP.
 - ii. Click OK to upload the file.
4. Click Close.
 5. Click Push Settings.

4.20.2 Activating Add-ons

If you have subscribed to the add-ons, URL Categorization, Risk Levels and/or Symantec AntiVirus services, you need to activate them.

In the Network Protection Licensing Portal (NPLP), do the following:

1. From the left menu, select Isolation > Software Add-on Activation.
2. Specify the VA Serial Number and the Activation Code^[1] that Symantec provided by email when you purchased the add-on.
3. Click Submit.

Note

The Symantec Threat Isolation Platform needs to be updated with the changes you made in the NPLP. This process takes a few minutes. When it is complete, you can start using the add-ons.

5 High Availability and Load Balancing

5.1 Overview

Maintaining High Availability (HA) and Load Balancing (LB) across multiple levels of components ensures quick response times from endpoint web browsers, as well as hardware and software redundancy within the Threat Isolation Gateways.

[1] In the order confirmation email, these add-ons may be referred to as: *BCIS Standard Web Security and Web Applications for SWG and *BCIS Advanced Web Security with Risk Controls and Web Applications for SWG.



5.2 High Availability and Load Balancing Process

To ensure High Availability (HA) and Load Balancing (LB), Symantec Threat Isolation maintains a multistage process with the following components:

- Proxy Auto-Configuration (PAC) file – See section [5.2.1 "Proxy Auto-Configuration \(PAC\) File"](#)
- Threat Isolation Proxy – See section [5.2.2 "Proxy"](#)
- Threat Isolation Engine (TIE) – See section [5.2.3 "Threat Isolation Engine \(TIE\)"](#)

For more information about Symantec Threat Isolation Platform components, see section [2.4 "Platform Components"](#)

5.2.1 Proxy Auto-Configuration (PAC) File

When a user initiates a browser session, a request is sent to a Proxy server to download the Proxy Auto-Configuration (PAC) file to the client PC. In order to maintain High Availability, multiple Proxies are recommended on the network. To add a new Threat Isolation Gateway, see section [4.7.7 "Defining a Threat Isolation Gateway"](#). Either a DNS is used to maintain availability and Load Balancing between multiple Proxies, or load balancing software, such as Ace or F5, is seamlessly integrated with Symantec Threat Isolation.

5.2.1.1 PAC File with DNS

The DNS will automatically choose the Proxy to download the current Proxy Auto-Configuration (PAC) file to the client browser. This process is external to the Symantec Threat Isolation application. Contact Symantec Threat Isolation technical support to update the DNS.

5.2.1.2 PAC File with External Load Balancing Software

All major external vendors that offer external load balancing software, including Ace and F5, can be seamlessly integrated to automatically select an appropriate Proxy to download the Proxy Auto-Configuration (PAC) file. For specific installation instructions, contact Symantec Threat Isolation technical support.



5.2.2 Proxy

A Naive Load Balancing Solution is utilized for Load Balancing and availability of the Threat Isolation Proxies. Listed within the Proxy Auto-Configuration (PAC) file is a list of Proxies to which the endpoint web browser or other user agents might connect. Utilizing an internal algorithm and the IP address from the client machine, the appropriate Proxy is accessed. When an endpoint browser attempts to access a Proxy that is busy, the PAC file array is accessed for another Proxy selection.

An internal monitoring system queries the Proxies to determine if they are in an available or non-available status. Any Proxy that is in a non-available status will be blocked from endpoint browser requests and PAC file download until it is available. If all Proxies are in a non-available status, an error will be displayed on the local browser. When any Proxy is in a non-working status, an error is notated in the Event Log.

5.2.3 Threat Isolation Engine (TIE)

The Threat Isolation Proxy communicates to the client browser which Threat Isolation Engine (TIE) server to use. An End-to-End Test simulates availability between the Proxy and the TIE server utilizing connectivity in port 443, and port 80 in HTTP/S mode. If the End-to-End Test fails, the TIE server is designated as non-available and the Event Log is updated.

The TIE also maintains an Internet Connectivity Test to ensure that access to the Internet is always available. If Internet access is not available, the TIE server is designated as non-available and the Event Log is updated.

5.2.3.1 TIE Key Mechanisms

Four key mechanisms interact to maintain consistent availability and Load Balancing between multiple Threat Isolation Engine (TIE) servers.

- TIE server list of available servers for client requests and network connections to the current host.
- Blacklist of TIE servers that failed to connect within a recent time frame session.
- Failover – An automatic rollover to a different TIE server if the current TIE server is no longer available.
- Stickiness – The client browser always returns to the primary TIE server for communication after any failover situation.



5.2.3.2 TIE Server List

The client receives a continuously updated list, or data store, of available and non-available Threat Isolation Engine (TIE) servers. The client maintains this data store locally and it is available for all browser requests. During the first session of the client computer to the TIE server, a primary TIE server is established. All cookies and downloads are maintained on the primary TIE server.

5.2.3.3 Blacklist

Within the Threat Isolation Engine (TIE) server list is a blacklist key. Any TIE server that fails to connect to the network is designated on the client blacklist and is no longer available for browser access. A continuous ping to all TIE servers ensures that the current status is accurate. If a client is connected to a TIE server that has lost network connectivity or has gone into non-available status, the client will automatically be routed to another TIE server via the failover mechanism.

5.2.3.4 Failover

Failover is an automatic rollover to a different Threat Isolation Engine (TIE) server if the current TIE server is blacklisted. If a failover occurs during an active session, the client computer displays a message stating "Reconnect in X seconds", where X counts down the seconds until service is restored via a new TIE server. When the new connection is established, the client must log in to the new browser connection.

Each tab on the browser establishes its own connection, and only the active tab requires a new client login. If the user switches to a different tab and the primary TIE server is still not available, the user will have to log in. Alternatively, if the primary TIE server becomes available before the user selects a new tab, there is no need to log in as all the cookies and downloads are current. If no servers are available, the client attempts to establish a connection to a random server. The new server becomes the primary server.

5.2.3.5 Stickiness

In the event of a failover, the client always attempts to reconnect with the primary Threat Isolation Engine (TIE) server when the server becomes available. This stickiness ensures that all cookies and downloads are maintained on one TIE server. When a browser tab that accessed another TIE server due to a failover is not active for two hours, it will automatically attempt to reconnect to the sticky, primary TIE server when the server is available. When a client refreshes their browser session or changes the URL, it will revert back to the sticky, primary TIE server when the server is available. This reconnection to the sticky, primary server is transparent to the end user.



6 Reports

6.1 Activity Logs and Analytics

The Reports heading in the Symantec Threat Isolation Management UI provides the following functionality:

- Activity Logs – Displays activity log tables and analytics widgets that draw from the same log data, and provides extensive search and filtering capabilities.
- Analytics – Includes a variety of analytics widgets that graphically display the same set of activity log data presented in the Logs tab.
- Report Servers – A list of existing report servers, and the option of adding new report servers.
- Log Forwarding – Forwarding of activity logs to Syslog, ArcSight and/or Apache Kafka for additional Information Management (IM). Forwarding of Management/Gateway audit logs to Syslog only.

6.1.1 Understanding the Activity Logs Window

Symantec Threat Isolation provides activity logs for all end-user browser activities taking place in the system. The Activity Log Profile (see section [4.3.6 "Defining Activity Log Profiles"](#)) associated with the organization's Symantec Threat Isolation security policy determines the depth of activities logged by the Symantec Threat Isolation system.

- To access the Activity Logs window, go to:



Reports → Activity Logs

The Activity Logs window consists of the areas described in the following table. The number next to each area corresponds to the same number in the screen capture, below.







#	Area	Description
Left side of window		
1	Logs tab	<ul style="list-style-type: none">■ Presents the log table and all log data■ This tab and the Analytics tab are linked to the same log data. Both tabs update automatically based on search parameters and filters set in either tab
2	Analytics tab	<ul style="list-style-type: none">■ Presents a number of analytics widgets that provide graphic views of the same data presented in the Logs tab■ This tab and the Logs tab are linked to the same log data. Both tabs update automatically based on search parameters and filters set in either tab



#	Area	Description
3	Narrow By	<ul style="list-style-type: none">■ Provides the most-searched values, grouped by field, and ordered by the largest number of log records■ Select one of the following filtering options:<ul style="list-style-type: none">◆ The Σ icon to display the numeric occurrences (absolute values) within the group◆ The % icon to display the percentage of occurrences (percent values) within the group◆ The  icon to add, remove, or reorder the filter selections■ Search is activated by checking one or more value checkboxes■ Topics include:<ul style="list-style-type: none">◆ Action◆ Component◆ Website◆ Categories◆ Etc.■ The operator for multiple checked value boxes within a field is OR■ The operator for multiple checked values over multiple fields is AND
4	Your Selections	<ul style="list-style-type: none">■ Lists filters activated for this search■ Presents all topics checked in the Narrow By area (see 3)
5		Toggle button that hides and opens the left-side search area
Top row of main window		
6	Severity Column	<ul style="list-style-type: none">■ Marks items that are critically important■ Check the Details column for additional information
7	Search	<ul style="list-style-type: none">■ Smart search field, opens a list of fields as you type■ Supports searching based on multiple fields and values■ Choose a field to open a list of values■ The operator for multiple search entries is always AND■ The operator for multiple search entries and date/time entries is AND■ Also supports free text searches■ Click the search icon to run a search■ Searching on a field produces results that also include all values
8	Date/time filters	<ul style="list-style-type: none">■ Date/time search field■ Click the bottom right corner to open a drop-down list of date search options■ Default date search is 7 days■ Choose Custom Search from the drop-down list to open a date/time search area



#	Area	Description
9	Reset	Reset button resets search to default search results
Relevant only to the Logs tab:		
10	Export	<ul style="list-style-type: none">■ Export button exports search results to a CSV file■ CSV output column headings are raw text titles
11		Traffic view button displays search results as a flat list
12		Session view button displays search results grouped by session
13		<ul style="list-style-type: none">■ Advanced settings for the Activity Logs
14		<ul style="list-style-type: none">■ Click to open a list of columns that can be displayed in the log table■ Select or clear column names depending on which columns you want displayed in the table
15		Click to display more values

6.1.2 Understanding the Logs Tab

6.1.2.1 Activity Logs Table Views

The activity logs table offers two different views:

- Traffic view - click the Traffic view button in the upper-right corner:



This view presents a flat list of all browser events, without the context of other events to which they might be related. Each entry in the table signifies a single event. The Session ID column lists the session ID of each event. This list includes data logged by all Threat Isolation Proxies and Threat Isolation Engines (TIEs), according to the Activity Log profile defined in section [4.3.6 "Defining Activity Log Profiles"](#).

#	Timestamp	Gateway	Event	Source IP	Username	Resource URL	Categories	Destination IP	Rule Nam...	Website URL	Sess...	Details
1	Oct 20, 16:08:14	eyal-Virt...	Network Request	192.168.56.1		e.nexac.com/e/ref...	Personal SL...	52.27.240.208	Allowed S...	www.thinkbroadband.c...	030_1	
2	Oct 20, 16:05:36	eyal-Virt...	Network Request	192.168.56.1		www.thinkbroadba...	Shopping, C...	80.249.99.130	Allowed S...	www.thinkbroadband.c...	879_1	
3	Oct 20, 16:03:06	eyal-Virt...	Network Request	192.168.56.1		www.thinkbroadba...	Shopping, C...	80.249.99.130	Allowed S...	www.thinkbroadband.c...	729_1	
4	Oct 20, 16:02:58	eyal-Virt...	Network Request	192.168.56.1		ams1-lb.adrxs.com...	Business	185.33.222.60	Allowed S...	www.thinkbroadband.c...	719_1	
5	Oct 20, 16:01:26	eyal-Virt...	Network Request	192.168.56.1		www.thinkbroadba...	Shopping, C...	80.249.99.130	Allowed S...	www.thinkbroadband.c...	629_1	
6	Oct 20, 16:00:29	eyal-Virt...	Network Request	192.168.56.1		ams1-lb.adrxs.com...	Business	185.33.222.170	Allowed S...	www.thinkbroadband.c...	569_1	
7	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		csp.mediaplex.com...	Business	64.156.167.98	Allowed S...	www.thinkbroadband.c...	480_1	
8	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	480_1	
9	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	480_1	
10	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	480_1	
11	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	480_1	
12	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	480_1	
13	Oct 20, 15:59:04	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	480_1	
14	Oct 20, 15:58:29	eyal-Virt...	Network Request	192.168.56.1		ams1-lb.adrxs.com...	Business	185.33.220.59	Allowed S...	www.thinkbroadband.c...	449_1	
15	Oct 20, 15:58:05	eyal-Virt...	Network Request	192.168.56.1		vap5iad3.lyjt.com/i...	Advertisem...	67.217.177.158	Allowed S...	www.thinkbroadband.c...	419_1	
16	Oct 20, 15:58:05	eyal-Virt...	Network Request	192.168.56.1		secure.fastclick.net...	Advertisem...	63.215.202.65	Allowed S...	www.thinkbroadband.c...	419_1	
17	Oct 20, 15:58:04	eyal-Virt...	Network Request	192.168.56.1		ce.lyjt.com/merge?...	Advertisem...	169.55.70.227	Allowed S...	www.thinkbroadband.c...	419_1	
18	Oct 20, 15:57:22	eyal-Virt...	Network Request	192.168.56.1		secure.img-cdn.me...	Business	92.122.131.182	Allowed S...	www.thinkbroadband.c...	379_1	
19	Oct 20, 15:57:04	eyal-Virt...	Network Request	192.168.56.1		ap.lyjt.com/contain...	Advertisem...	67.217.177.158	Allowed S...	www.thinkbroadband.c...	359_1	
20	Oct 20, 15:57:04	eyal-Virt...	Network Request	192.168.56.1		lb.adrxs.com/asyn...	Advertisem...	185.33.220.215	Allowed S...	www.thinkbroadband.c...	359_1	
21	Oct 20, 15:54:02	eyal-Virt...	Network Request	192.168.56.1		pixel-a.sitescout.co...	Advertisem...	66.155.15.42	Allowed S...	www.thinkbroadband.c...	180_1	
22	Oct 20, 15:54:02	eyal-Virt...	Network Request	192.168.56.1		d.chango.com/m...	Advertisem...	208.43.247.70	Allowed S...	www.thinkbroadband.c...	180_1	

Showing 23 out of 23 matching records

- Session view - click the Session view button in the upper-right corner:



This view presents sessions and their related resources. A session consists of the URL address entered by the end user in the address bar of the browser, along with all additional session resources that make up that webpage, such as ads, pictures, and so on. The Session view consists only of data logged by all TIEs.

While most log views offer only a list of traffic that flows through a Threat Isolation Gateway, Session view offers a unique log display that tracks what the user requested as well as who requested the information. Frequently, the website requests information to display that is a byproduct of an additional request of the original URL. Utilizing the Isolation session, you can determine the true origin of everything on the browser. This offers a new level of detail that is new to the security industry.

#	Timestamp	Gateway	Event	Source IP	Username	Resource URL	Categories	Destination IP	Rule Name	Details
1	Mar 2, 12:06:33	dev	(24 records)	192.168.56.1	jessiecor...	www.findmyphoneapplesup...	Unknown/U...	142.0.34.21	Allowed S...	Session
1.1	Mar 2, 12:06:35	dev	Tab Close	192.168.56.1	jessiecor...	www.findmyphoneapplesup...	Unknown/U...	142.0.34.21	Allowed S...	Session Resources
1.2	Mar 2, 12:06:36	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphoneapplesup...	Unknown/U...	142.0.34.21	Allowed S...	
1.3	Mar 2, 12:06:36	dev	Network Request	192.168.56.1	jessiecor...	ajsoftsolutions.com/script2.js	Unknown/U...	54.172.161.218	Allowed S...	
1.4	Mar 2, 12:06:36	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphoneapplesup...	Unknown/U...	142.0.34.21	Allowed S...	
1.5	Mar 2, 12:06:36	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphoneapplesup...	Unknown/U...	142.0.34.21	Allowed S...	
2	Mar 2, 12:06:24	dev	(21 records)	192.168.56.1	jessiecor...	www.findmyphone.com/login...	Unknown/U...	142.0.34.21	Allowed S...	Blocked phishing attempt.
2.1	Mar 2, 12:06:32	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphone.com/login...	Unknown/U...	142.0.34.21	Allowed S...	Blocked phishing attempt.
2.2	Mar 2, 12:06:30	dev	Keyboard	192.168.56.1	jessiecor...	www.findmyphone.com/	Unknown/U...	142.0.34.21	Allowed S...	
2.3	Mar 2, 12:06:25	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphone.com/img/s...	Unknown/U...	142.0.34.21	Allowed S...	
2.4	Mar 2, 12:06:25	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphone.com/img/i...	Unknown/U...	142.0.34.21	Allowed S...	
2.5	Mar 2, 12:06:25	dev	Network Request	192.168.56.1	jessiecor...	www.findmyphone.com/img/2...	Unknown/U...	142.0.34.21	Allowed S...	
3	Feb 25, 08:56:53	dev	(40 records)	192.168.30.98	craigice@...	www.zwsoft.com/index.php?...	Computers...	50.23.196.186	Allowed S...	Session
3.1	Feb 25, 08:56:59	dev	Tab Close	192.168.30.98	craigice@...	www.zwsoft.com/index.php?...	Computers...	50.23.196.186	Allowed S...	Session Resources
3.2	Feb 25, 08:56:54	dev	Network Request	192.168.30.98	craigice@...	www.zwsoft.com/statics/ima...	Computers...	50.23.196.186	Allowed S...	
3.3	Feb 25, 08:56:54	dev	Network Request	192.168.30.98	craigice@...	www.zwsoft.com/statics/ima...	Computers...	50.23.196.186	Allowed S...	
3.4	Feb 25, 08:56:54	dev	Network Request	192.168.30.98	craigice@...	www.zwsoft.com/statics/ima...	Computers...	50.23.196.186	Allowed S...	
3.5	Feb 25, 08:56:54	dev	Network Request	192.168.30.98	craigice@...	www.zwsoft.com/statics/ima...	Computers...	50.23.196.186	Allowed S...	
4	Feb 25, 08:56:50	dev	(2 records)	192.168.30.98	craigice@...	www.zwsoft.com/index.php?...	Computers...	50.23.196.186	Allowed S...	

Notes

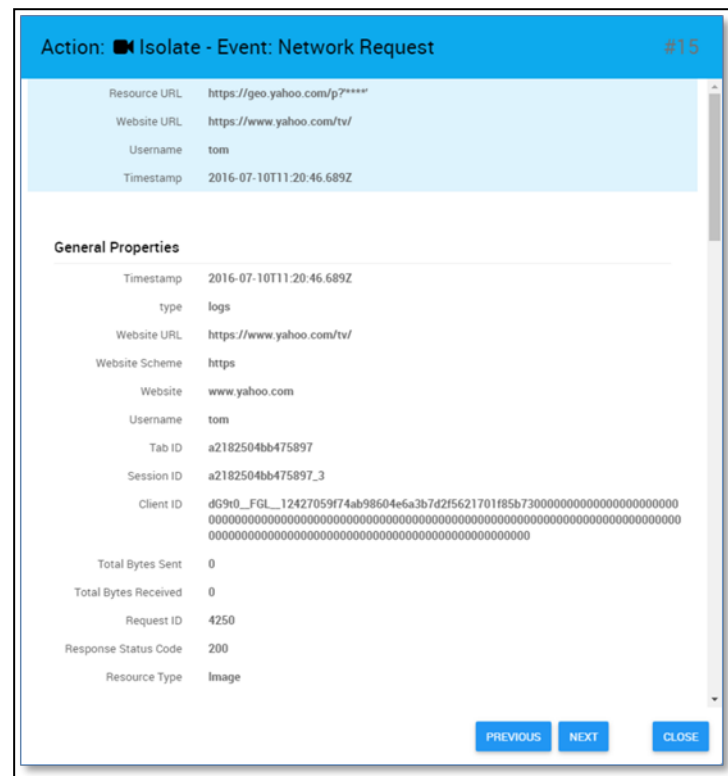
- The results of a search performed from either tab (Logs or Analytics) are automatically displayed in the other tab, as well.
- All Activity Logs tables have a continuous scroll feature that allows you to scroll down through all results



6.1.2.2 Activity Log Event Window

1. To access the Activity Log Event window for an individual event, click the timestamp associated with one of the events.

The Event window opens, as shown below.



The Event window contains a detailed list of parameters for which the system gathers data for each event. The parameters are grouped as follows:

- ◆ General Properties
- ◆ Event Properties
- ◆ Source
- ◆ Destination
- ◆ Isolation Network Statistics
- ◆ Categories
- ◆ Parent Categories
- ◆ User Groups
- ◆ Rule



- ◆ Resource Response Headers
 - ◆ Resource Request Headers
 - ◆ Endpoint Properties
 - ◆ Destination Geolocation
 - ◆ Miscellaneous
2. To display the actual log structure logged for the event, click the Show Raw Data button. (The raw data parameter names are the displayed column headings when you export the log data to a CSV file.)

6.1.3 Understanding the Analytics Tab

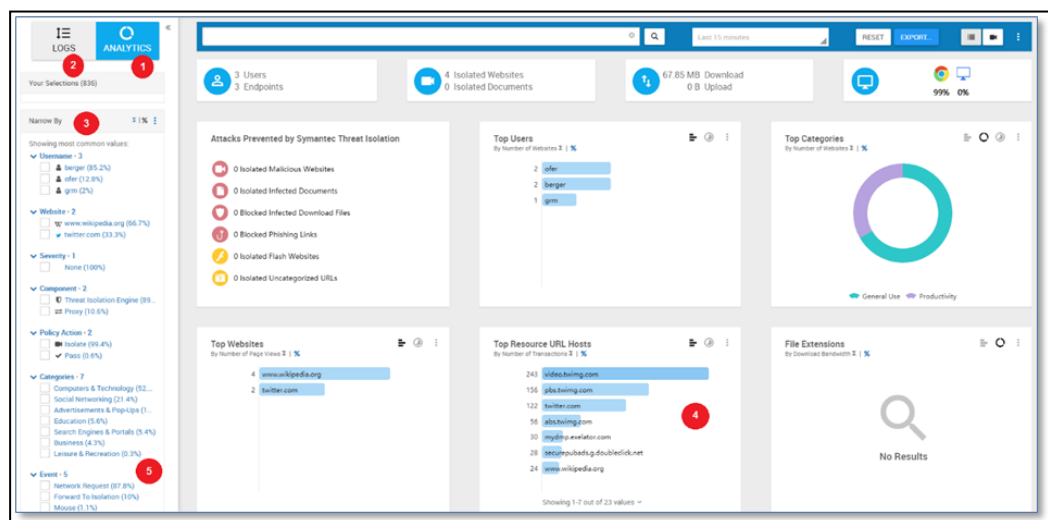
The Analytics tab includes a variety of analytics widgets that display the same set of activity log data presented in the Logs tab, by means of visual images.

Note

The results of a search performed from either the Logs tab or the Analytics tab are automatically displayed in the other tab as well.





To access the Analytics tab from the Management UI, go to one of the following:

- Reports → Activity Logs → Analytics
- Reports → Analytics








The Analytics tab, shown above, consists of the areas listed in the following table. The number next to each area corresponds to the same number in the screen capture.






#	Area	Description	For More Information
	Analytics tab	<ul style="list-style-type: none">■ Presents a number of analytics widgets that provide a graphic view of the same data that is presented in the Logs tab■ The Analytics tab and the Logs tab are linked to the same log data. Both tabs update automatically based on search parameters and filters set in either tab	
	Logs tab	<ul style="list-style-type: none">■ Presents the log table and all log data■ The Logs tab and the Analytics tab are linked to the same log data. Both tabs update automatically based on search parameters and filters set in either tab	
	Narrow By	<ul style="list-style-type: none">■ Provides the most-searched values, grouped by field and ordered by the largest number of log records■ Select one of the following:<ul style="list-style-type: none">◆ Σ for numeric occurrences within the group◆ % to display the percentage of occurrences within the group◆  to add, remove or reorder the filter selections■ Search is activated by checking one or more value checkboxes■ Topics include:<ul style="list-style-type: none">◆ Action◆ Component◆ Website◆ Categories◆ Etc.■ The operator for multiple checked value boxes within a field is OR■ The operator for multiple checked values over multiple fields is AND >	



#	Area	Description	For More Information
	Values	<ul style="list-style-type: none">■ Click any value in a widget to display a context menu■ Menu options vary depending on the selected value and the current display type (bar, pie or timeline)	"Filtering by Analytics categories", below in this section
		Click to display more values	

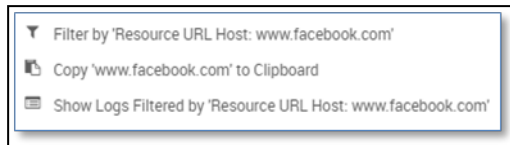
Widget Display Types

The rest of the window contains Analytics widgets. For each widget, you can choose the display types described in the following table.

Icon	Description
	Bar graph
	Pie chart
	Timeline
	Measure By options, enables you to order the data in an analytics widget in a specific order without affecting other widgets.
	Export results to a PDF NOTE: By default, the PDF will contain the top 200 results. You can modify this number in the Activity Logs Advanced Settings dialog. For more information, see section 6.2.6 "Filtering Using the Advanced Settings" .

Filtering by Analytics Categories

You can filter on any category listed in the widgets by clicking any value on which you want to filter log data. A menu list opens that includes the following filter choices:

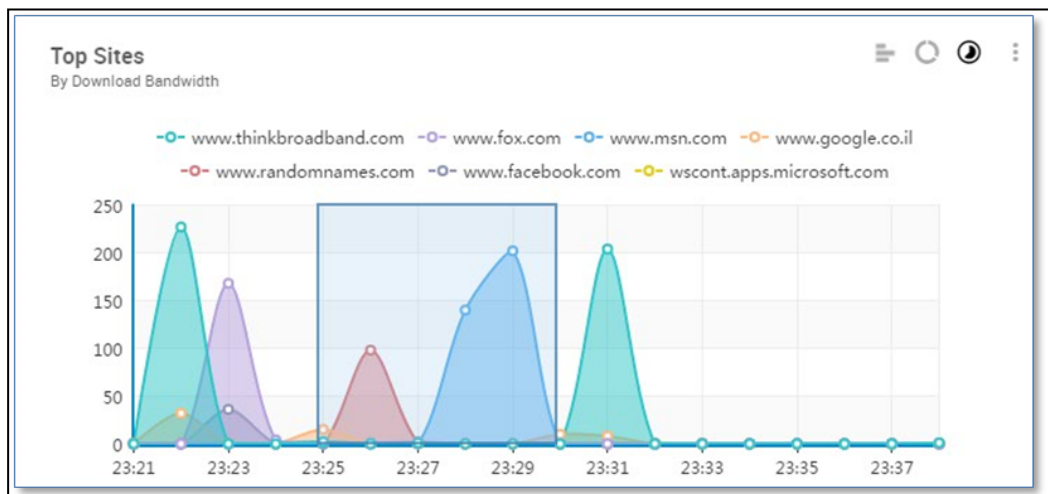


- Filter by <field name: field value> – Filters based on your choice of field and value, and updates all widget displays.
- Show Logs Filtered by <field name: field value> – Filters based on your choice of field and value, and opens the Logs tab with updated results.



- Zoom In by <field name: field value> – Filters based on your choice of field and value, and updates only that widget. This option is available only with certain widgets.

You can also filter down levels within a category: In timeline view, drag and drop the mouse in the timeline area to zoom in by time. Filtering takes place and the new, smaller range of data is presented in both the Logs and Analytics tabs.





6.2 Filtering and Searching Logged Data

There are several ways to filter logged data that are available from both the Logs and Analytics tabs:

- Using the search bar
- Using the time field
- Using the filters in the Narrow By area on the left side of the window
- Using the follow session option

All of these filtering methods affect the displayed data in both the Session View tab and the Traffic View tab. You can use the back button and forward button on your browser to undo and redo your filtering actions.

6.2.1 Filtering Using the Search Bar

1. Click the search bar at the top of the page.
A drop-down menu opens with a list of fields.

2. Click one of the fields.
A list of categories opens.

3. Choose the value on which you want to filter.
The search option supports the logical operators AND, OR, NOT, and parenthesis. You can choose multiple fields and values for filtering to further narrow your search results.

6.2.2 Filtering Using the Time Field

1. To filter within a specific time range, click the time bar at the top of the Activity Logs window.




2. Choose an option.
If you choose Custom Range, a double calendar window opens.
3. Set the start and end times and dates.
4. Click Apply.



The log data is filtered based on your custom time range.

6.2.3 Filtering Using the Narrow By Area

A variety of filtering options is available in the Narrow By area on the left side of the Activity Logs window. Out of the box, Symantec Threat Isolation provides a dozen filters. Changes to the filtering options are reflected immediately in the activity logs table.

1. Select one of the following filtering options:
 - ◆ The Σ icon, to display the numeric occurrences (absolute values) within the group
 - ◆ The % icon, to display the percentage of occurrences (percent values) within the group
 - ◆ The  icon, to add, remove, or reorder the filter selections
2. Scroll up and down and choose the categories on which to filter.

6.2.4 Filtering Using the Follow Session Option

Filtering by using the Follow Session option offers a unique display that enables the Management user to track an individual browsing session and follow each web address that the browser accesses. This provides a level of organizational detail that is new to the security industry.


1. To enable Follow Session, right-click the row of the session that you want to follow.
2. Select Follow Session.

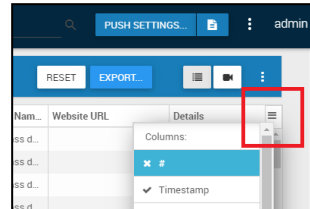
To return to the Activity Logs window, select Undo at the bottom right of the screen, or click the Back button on the browser.

6.2.5 Filtering by Displaying or Hiding Specific Columns

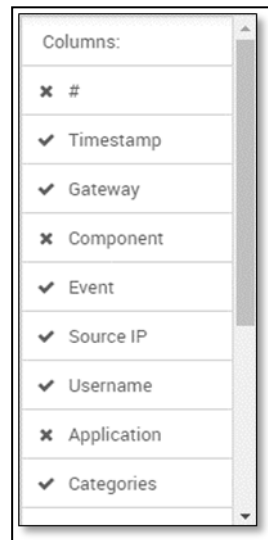
This method of filtering is accessible only from the Logs tab.




1. Click the  icon in the upper right corner of the Logs table to open the Columns drop-down list.

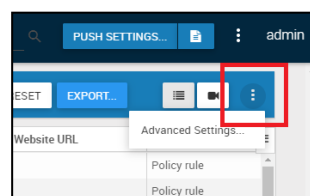


2. Click a column in the drop-down list to display it; click it again to hide it. A displayed column is preceded by ✓; a hidden column is preceded by ✕.



6.2.6 Filtering Using the Advanced Settings

1. To access the Activity Log Advanced Settings, click the icon  on the far right of the search bar.



2. Configure the parameters described in the table below, and then click Update.



Parameter	Description	For More Information
Search Properties		
Default Time Range	The default amount of time displayed on the activity log	
Default View	Select either: <ul style="list-style-type: none">■ Session View■ Traffic View	See section 6.1.2.1 "Activity Logs Table Views" for detailed information about Session and Traffic Views
Search Bar Options	By selecting Instant Results As You Type, the results field is continuously updated while you type in the search field	
Export Limits		
Logs	The maximum number of log records to export to the CSV file. Download limit is 30000 entries	See section 6.2.7 "Exporting Logged Data to CSV"
Analytics Widgets	The number of results included in the PDF. Default: 200	See section 6.2.8 "Exporting Logged Data to PDF"
Filters Widgets	The number of results included in the PDF. Default: 200	See section 6.2.8 "Exporting Logged Data to PDF"
Session View Properties		
Preview Records	The maximum number of preview records to be displayed	

6.2.7 Exporting Logged Data to CSV

Symantec Threat Isolation allows you to export logged data to a CSV file. This is useful when you want to export search results and view all fields together in a spreadsheet.

- To export logged data to a CSV file that is readable in Excel, click the Export button in the upper right corner of the screen, above the Activity Log table.

All log data is exported to the CSV file.

Note

The column headings are taken directly from the log entry code and are not necessarily the same friendly headings seen in the online log table.

By default, the maximum number of log entries that Symantec Threat Isolation allows you to export to a CSV file is 30000. To export more than this number, you



can implement a client that consumes the Management API to search for logs, using the Management API `/trafficreports/generate/requests`. Note that this must be done using the pagination method the API provides. The client code fetches as many logs as needed, and then exports them to a CSV file or a file of any other format.

The Management APIs are documented in the *Symantec Web Isolation Management API Guide*. To receive a copy of this API guide, contact Symantec technical support.

6.2.8 Exporting Logged Data to PDF

Symantec Threat Isolation allows you to export logged data that is displayed in a specific "Narrow By" filter or Analytics widget, to a PDF file. This is useful when you want to view many results together.

1. Do one of the following:

- ◆ To export logged data that is displayed in a specific "Narrow By" filter, click the download button next to the filter:



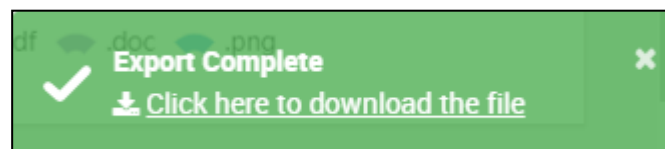
- ◆ To export logged data that is displayed in an Analytics widget, click the download button at the top of the widget:



Note

By default, the top 200 results are exported. You can modify this number in the Activity Logs Advanced Settings dialog. For more information, see section [6.2.6 "Filtering Using the Advanced Settings"](#)

2. When the export is complete, the following message appears at the bottom of the page:



3. Click the link to download the PDF.



6.3 Defining a Report Server

To be able to use the Symantec Threat Isolation activity logs, you must first define the report server from which the report data will be accessed.

Note

This procedure is relevant only if the report server was not activated when you defined the Management Gateway, or if a report server that was deleted needs to be recreated.

1. To create a report server, go to:
Reports → Report Server → New Report Server
2. Specify the hostname of the new report server and a relevant comment, and then click Create.

Currently, the hostname must be 169.254.0.1.

For information about enabling the report server, see section [3.5.7 "Defining the Management Gateway"](#), step 12.

6.4 Log Forwarding

All defined activity logs are stored in the Symantec Threat Isolation Report Server, defined as explained in section [6.3 "Defining a Report Server"](#). For additional information management utilizing Security Information and Event Management (SIEM), activity logs can be forwarded to Syslog, ArcSight and/or Apache Kafka management systems. The Log Forwarding object is created during installation and must be updated with the appropriate server name(s) to become active.

6.4.1 Configuring Log Forwarding

You can configure your system to forward Symantec Threat Isolation activity logs, Management audit logs, and Threat Isolation Gateway audit logs to external log servers.

1. To configure log forwarding to external log servers, go to:
Reports → Log Forwarding
2. Click Edit.
3. Configure the parameters described in the following table, and then click Update to activate the log forwarding configuration.

Parameter	Description	For More Information
Destination Servers		



Parameter	Description	For More Information
Activity Logs	Select Syslog, ArcSight and/or Apache Kafka server(s)	<ul style="list-style-type: none">■ For Syslog servers, see section 4.13 "Configuring SNMP Servers"■ For ArcSight servers, see section 4.15 "Configuring ArcSight Servers"■ For Apache Kafka servers, see section Configuring Apache Kafka Servers
Management Audit Logs	Select Syslog server(s)	For Syslog servers, see section 4.13 " Configuring SNMP Servers "
Gateway Audit Logs	Select Syslog server(s)	For Syslog servers, see section 4.13 " Configuring SNMP Servers "

7 Monitoring

Symantec Threat Isolation maintains extensive event logs for system events. The Management User has the option to adjust metric thresholds for even greater tracking of logged events. Monitor Groups are used to organize Threat Isolation Gateway thresholds, event logs and message alerts.

7.1 Event Logs

The Symantec Threat Isolation Event Log displays all system events in descending order, with the newest events at the top of the list and older ones listed as you scroll down.

- To configure the Event Log, go to:

Monitoring → Event Logs

Event Log						
Showing most recent system events						
#	Timestamp	Gateway	Source	Event	Severity	Details
1	Jul 31, 09:41:16	gw.organization.d...	Metric Threshold	Recovered	Critical	Metric Threshold "No Open Tabs" is back to normal (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold...
2	Jul 31, 09:22:05	gw.organization.d...	Metric Threshold	Triggered	Critical	Metric Threshold "No Open Tabs" is failing (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold: 1 for 19...
3	Jul 31, 09:20:34	gw.organization.d...	Metric Threshold	Recovered	Critical	Metric Threshold "No Open Tabs" is back to normal (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold...
4	Jul 31, 08:11:54	gw.organization.d...	Metric Threshold	Triggered	Critical	Metric Threshold "No Open Tabs" is failing (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold: 1 for 23...
5	Jul 31, 08:09:53	gw.organization.d...	Metric Threshold	Recovered	Critical	Metric Threshold "No Open Tabs" is back to normal (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold...
6	Jul 30, 21:54:43	gw.organization.d...	Metric Threshold	Triggered	Critical	Metric Threshold "No Open Tabs" is failing (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold: 1 for 21...
7	Jul 30, 21:53:12	gw.organization.d...	Metric Threshold	Recovered	Critical	Metric Threshold "No Open Tabs" is back to normal (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold...
8	Jul 30, 21:41:06	gw.organization.d...	Metric Threshold	Triggered	Critical	Metric Threshold "No Open Tabs" is failing (Metric: fireglass_tabs_count, Reason: Metric was lessThan defined threshold: 1 for 20...

The Event Log displays the parameters described in the table below.

**Table 9 Event Log columns**

Parameter	Description
# (Number)	A unique identifier number
Timestamp	The date and time of the event
Gateway	The Threat Isolation Gateway that reported the event
Source	The threshold that initiated the event
Event	Whether the event triggered or recovered from a metric threshold <ul style="list-style-type: none">■ Triggered - Event that reached the metric threshold■ Recovered - Event that reverted to within the metric threshold range
Severity	The event's level of severity: Critical, High, Medium or Low
Details	The metric threshold and the reason for the event

7.2 Monitor Groups

Monitor Groups enable you to select multiple metric thresholds and Threat Isolation Gateways, setup email alerts, as well as Syslog and SNMP servers to forward the specified event logs.

During installation, an initial Monitor Group object is created and must be updated with the email and Syslog/SNMP server names. After log forwarding settings are updated (see section [6.4.1 "Configuring Log Forwarding"](#)), email alerts and event log information is forwarded to the Syslog/SNMP servers for the specified group.

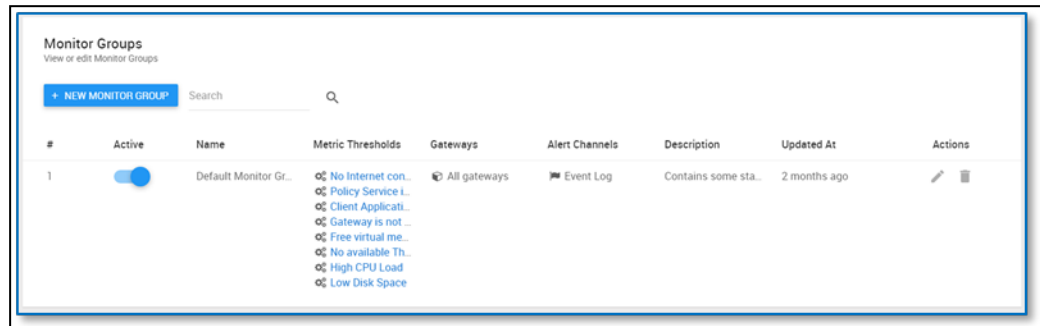
The following metric thresholds are included in this initial monitor group:

- No Internet connectivity
- Async services is down
- Resource server is down
- Gateway is not alive
- Free virtual memory too low
- No available application servers
- No open tabs
- High CPU load
- Low disk space



1. To configure a new Monitor Group, go to:

Monitoring → Monitor Groups → New Monitor Group



2. Configure the parameters described in the table below for the new Monitor Group, and then click Create.

Parameter	Description	Additional Information
Metric Thresholds	Select the metric thresholds for this Monitor Group	
Gateways	Select the Gateways for this Monitor Group	
Email Servers	Select the email servers for this Monitor Group	
Syslog Servers	Select the Syslog servers for this Monitor Group	
SNMP Servers	Select the SNMP servers for this Monitor Group	
Alert Logging	Specifies if alert logs are sent to the event log	Default: Log alerts to the event log
Active	Specifies if the Monitor Group is active	Default: Active

7.3 Metric Thresholds

Threat Isolation Gateways send both system metrics, such as disk status, CPU status and so on, and application metrics to the Management server using the metric threshold mechanism. The Management server collects these metrics, and when a metric threshold is crossed, it sends both system metrics and application metrics to the SNMP server via SNMP traps. The standard Linux MIB is exposed; the top level of the MIB's OID is .1.3.6.1.2.1.1.

A metric threshold is a preset limit based on system considerations, such as high CPU load or low disk space. When this limit is reached, an event can be set up to



notify the Management user, and logs are created for auditing and tracking. Out of the box, Symantec Threat Isolation is preconfigured with dozens of metrics. You can change or extend the preset metrics according to your needs.

The following preset metrics are available to update the thresholds for event logging. These preset metrics might be updated or changed for future versions:

- No Internet connectivity
- Policy Service is down
- Client application service is down
- Gateway is not alive
- Free virtual memory is too low
- No available Threat Isolation Servers
- High CPU load
- Low disk space

1. To configure a metric threshold, go to:

Monitoring → Metric Thresholds → New Metric Threshold

#	Name	Description	Metric	Updated At	Actions
4	No Internet connectivity	Alert when there is no Internet connectivity for 75% of the samples (System Created)	fireglass_internet_access_status is less than 1 for 90 seconds	2 months ago	Edit Delete
5	Policy Service is down	Alert when Policy Service is not responsive for 75% of the samples (System Created)	fireglass_policy_service_status is less than 1 for 90 seconds	2 months ago	Edit Delete
6	Client Application Service is down	Alert when the Client Application Service is not responsive for 75% of the samples (System Created)	fireglass_resource_access_status is less than 1 for 90 seconds	2 months ago	Edit Delete
7	Gateway is not alive	Alert when the gateway is not responding properly for 75% of the samples (System Created)	fireglass_gateway_heartbeat_status is less than 1 for 90 seconds	2 months ago	Edit Delete
8	Free virtual memory too low	Alert when available virtual memory is below 100 mb (System Created)	system_memory_virtual_available is less than 100000000 for its lowest value	2 months ago	Edit Delete
9	No available Threat Isolation Engines	Send an alert when there have not been any available Threat Isolation Engines for 75% of the samples (System Created)	status_manager_available_application_servers is less than 1 for 90 seconds	2 months ago	Edit Delete

2. Configure the parameters described in the table below for the new metric threshold, and then click Update.



Parameter	Description	Additional Information
Metric Information		
Metric	The metric being monitored	Symantec Threat Isolation defines dozens of preconfigured metrics. For more a description of each metric, see the table below
Operator	Select the operator for the threshold. Options are: <ul style="list-style-type: none">■ Greater than■ Less than■ Equal to■ Unequal to	
Value	The value a threshold must meet to trigger an event	
Measurement Method	<ul style="list-style-type: none">■ Range of Time - The number of seconds the threshold must be met in order to trigger an event■ Function - The aggregator of the value of the metric threshold. Options are:<ul style="list-style-type: none">◆ Sum◆ Average◆ Lowest value◆ Highest value	All measurements are based on a 2-minute window to meet the threshold

The following table explains each preconfigured metric available from the Metric drop-down list.

Metric	Description	Possible Values
status_manager_available_vb_servers	The Gateway with a Proxy component has access to a TIE	1 - True 0 - False
system_cpu_system_wide_percent	Percentage of CPU usage system-wide	0 - 100
system_cpu_system_wide_times_percent_user	Percentage of time system-wide the CPU spent running user space processes	0 - 100
system_cpu_system_wide_times_percent_nice	Percentage of CPU usage system-wide, factoring in niceness	0 - 100



Metric	Description	Possible Values
system_cpu_system_wide_times_percent_system	Percentage of time system-wide the CPU spent running the kernel	0 - 100
system_cpu_system_wide_times_percent_idle	Percentage of time system-wide the CPU spent in an idle state	0 - 100
system_cpu_system_wide_times_percent_iowait	Percentage of time system-wide the CPU spent waiting for IO operations to complete	0 - 100
system_cpu_system_wide_times_percent_irq	Percentage of time system-wide the CPU spent handling Interrupts	0 - 100
system_cpu_system_wide_times_percent_steal	Percentage of time system-wide the CPU spent waiting for another virtual CPU to be serviced	0 - 100
system_disk_root_total	Total root disk size	Bytes
system_disk_root_used	Total root disk used	Bytes
system_disk_root_free	Total root disk free	Bytes
system_disk_root_percent	Total root disk usage percentage	0 - 100
system_memory_swap_total	Total memory swap size	Bytes
system_memory_swap_used	Memory swap size in use	Bytes
system_memory_swap_free	Memory swap size free	Bytes
system_memory_swap_percent	Memory swap size usage percentage	0 - 100
system_memory_virtual_total	Total size of virtual memory in the system	Bytes
system_memory_virtual_available	Total virtual memory free (plus buffers/cache)	Bytes
system_memory_virtual_used	Total virtual memory in use	Bytes
system_memory_virtual_free	Total virtual memory free	Bytes



Metric	Description	Possible Values
system_memory_virtual_percent	Total virtual memory free percentage	0 - 100
system_memory_virtual_buffers	Total virtual memory allocated to buffers	Bytes
system_memory_virtual_cached	Total virtual memory allocated to cache	Bytes
system_network_bytes_sent	Total number of bytes sent from the system	Bytes
system_network_bytes_recv	Total number of bytes received in the system	Bytes
system_network_packets_sent	Total number of packets sent from the system	Number of packets
system_network_packets_recv	Total number of bytes received in the system.	Bytes
system_network_errin	Total number of errors while receiving	Number of errors
system_network_errout	Total number of errors while sending	Number of errors
system_network_dropin	Total number of incoming packets that were dropped	Number of packets
system_network_dropout	Total number of outgoing packets that were dropped	Number of packets
fireglass_tabs_count	Number of Symantec Threat Isolation tabs open on the Gateway	Number of tabs
fireglass_active_tabs_count	Number of Symantec Threat Isolation tabs currently active on the Gateway	Number of active tabs
fireglass_user_count	Number of unique users on the current Gateway	Number of unique users
status_manager_test_results_success	Reports the results of system tests	1 - Success 0 - Failure
fireglass_internet_access_status	Reports Gateway Internet access	1 - True 0 - False
fireglass_policy_server_status	Reports status of policy service	1 - Online 0 - Offline



Metric	Description	Possible Values
fireglass_client_resource_server_status	Reports status of client resource service	1 - Online 0 - Offline
fireglass_proxy_life_status	Reports status of local ATS	1 - Online 0 - Offline
ldap_failures	Reports the number of LDAP access/connectivity errors that occurred recently	Number of LDAP errors
fireglass_gateway_heartbeat_status	Reports status of Gateway's communication to Management	1 - Online 0 - Offline
status_manager_available_application_servers	Reports the number of running Threat Isolation Servers	Number of application servers

The following is an example of a High CPU Load metric threshold. In this example, an event log will be created when the average system CPU load is greater than 90%.

Create Metric Threshold

General

Name

Description

Metric Information

Metric
System wide CPU usage percentage

Operator

Value

Measurement Method ☐ Range of time
☒ Function

Threshold is measured within a two minute window.



Each configured metric threshold can be included in the Monitor Group to coordinate the event logging and email notifications as a Group object.



8 User Experience

When utilizing the enhanced security features of Symantec Threat Isolation, the end user experiences slight differences between the standard interaction of the browser and the alternative Symantec Threat Isolation interaction. This section explains these differences.

8.1 Context Menu Display

Scenario

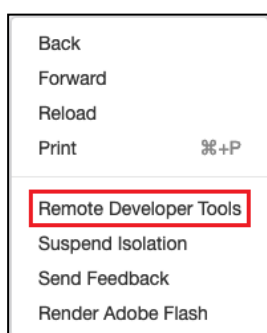
When the end user right-clicks on the browser, the context menu that is displayed is the browser's native menu. Using the default browser native menu lets the end user enjoy a seamless experience. To configure Symantec's custom context menu instead, see section [4.3.3.2 "Adding an Isolation Profile"](#). Regardless of which context menu is selected, the end user can display an Advanced Options screen by pressing Ctrl+Q. For more information about the Advanced Options screen, see section [4.3.3.2 "Adding an Isolation Profile"](#).

8.1.1 Custom Symantec Context Menu

The Symantec custom context menu differs slightly from the browser context menu. The options in the following sections are extra features which are not in the context menu by default.

8.1.2 Remote Developer Tools

For end users who work in Internet software development, easy access to browser developer tools is essential. Note that the Remote Developer Tools option is not displayed by default. To change the default settings, see section [4.3.8.3 "Opening Developer Tools Remotely"](#).

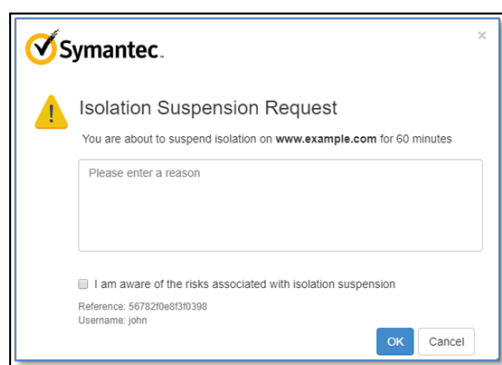
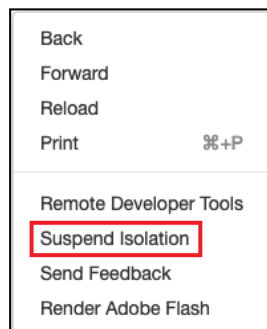




The Remote Developer Tools option can also be displayed from the Advanced Options screen. Note that the action is available from that screen only if it is enabled in the relevant settings. See section [4.3.3.2 "Adding an Isolation Profile"](#).

8.1.3 Suspend Isolation

Isolation ensures a safe web viewing environment. It is not recommended to suspend isolation. When an end user decides to use the native browser, they can select Suspend Isolation for the current website and continue browsing in Inspect mode. A warning message is displayed in a pop-up window; the end user is required to specify a reason for exiting the protected environment, and select a checkbox to confirm awareness of the risks associated with less secure browsing. For auditing purposes, a tracking ticket is created with the username, reference number and the website viewed. It can be easily found in the activity logs.



By default, the Suspend Isolation option is not displayed in the context menu. This option can be added to the browser context menu, and the active time of 60 minutes can be modified. For information about changing the default settings, see section [4.4.8 "Creating URL Objects and Object Groups"](#).



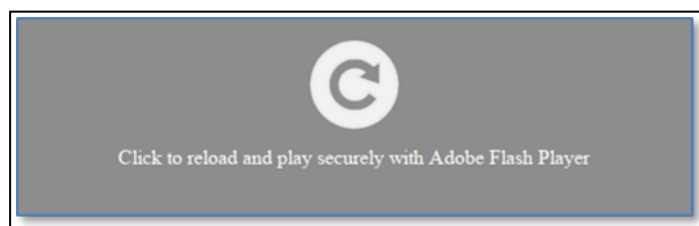
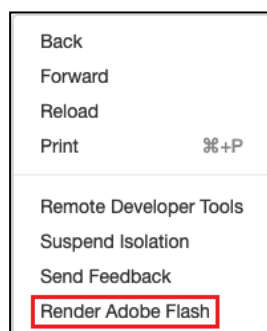
The Suspend Isolation option can also be displayed from the Advanced Options screen. Note that the action is available from that screen only if it is enabled in the relevant settings. See section [4.3.3.2 "Adding an Isolation Profile"](#).

8.1.4 Render Adobe Flash

On rare occasions when a webpage runs a Flash video, a message will be displayed, asking the end user to click the screen to view the video. This action enables the Adobe Flash plug-in and the video is loaded as expected within the browser. When an end user browses a website that uses a lot of Flash video, Render Adobe Flash can be selected from the context menu; while the user is on the current website's hostname and tab, all Flash video is enabled.

The Render Adobe Flash option can also be displayed from the Advanced Options screen. Note that this option is available only when Symantec Threat Isolation does not enable Flash rendering automatically in the browsed website. For more information, see section [4.3.3.2 "Adding an Isolation Profile"](#).

Flash functionality enables the playing of Flash media on the Symantec Threat Isolation Platform and not on the local machine. This adds an extra layer of security protection by offering Flash functionality that never runs on the local machine.



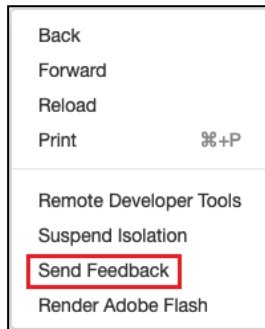
8.1.5 Send Feedback

End users who want to send feedback about any isolated or blocked webpage, can select Send Feedback from the context menu.



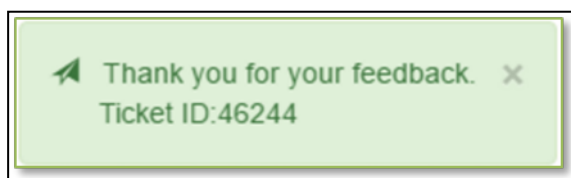
The Send Feedback option can also be displayed from the Advanced Options screen. Note that the action is available from that screen only if it is enabled in the relevant settings. See section [4.3.3.2 "Adding an Isolation Profile"](#).

A pop-up window is displayed. The user should specify their email address and a free text comment, and can select a checkbox to send a screen capture of the current browser screen (default) with the message.



A screenshot of a Symantec feedback form pop-up window. The window has a title bar with a close button. The Symantec logo is at the top left. Below it, the text reads: "Your feedback is welcome" and "Build: 1.9.0-alpha". The form contains a label "Fill in your Email and feedback:" followed by an "Email" input field and a "Feedback" text area. Below these is a checkbox labeled "Send a screenshot" which is checked. At the bottom right are "Send" and "Cancel" buttons.

After the user sends the feedback, a tracking number is displayed. The user is advised to write down this number for future reference. The number can be searched for in the activity logs.





By default, the Send feedback option generates an email to Symantec Threat Isolation, but the email address can be changed to that of the organization's IT department. For more information, see section [4.7.8 "Defining Gateway Advanced Settings"](#).

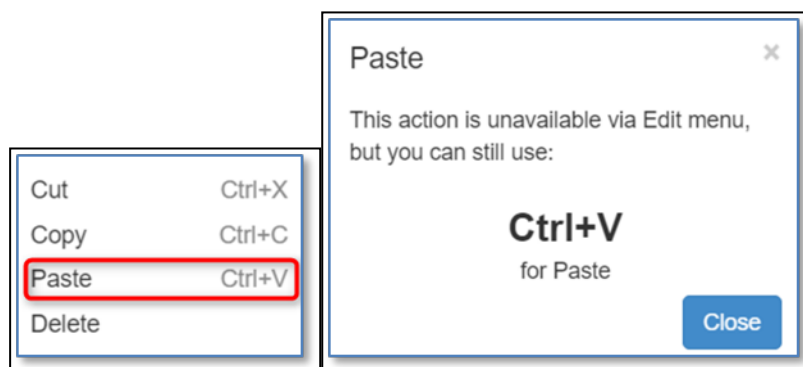
8.1.6 Cut, Copy and Paste

The cut and copy features are identical to those in the native browser experience. On rare occasions, a pop-up window is displayed and advises the end user to use the following keyboard shortcuts.

Function	Keyboard Shortcut
Cut	Ctrl-X
Copy	Ctrl-C

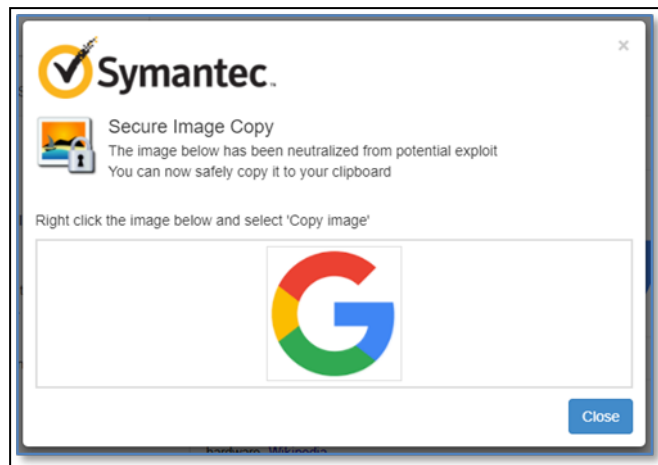
8.1.6.1 Paste Functionality

The paste functionality always requires the end user to use Ctrl+V.



8.1.7 Copy Image

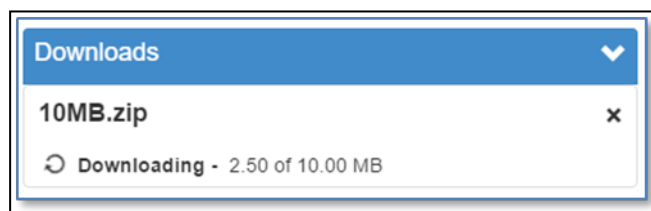
When a user copies an image using the context menu, a pop-up window is displayed to ensure that the image has been neutralized from potential exploits. The end user is instructed to right-click the displayed image and select Copy image to complete the process.



8.2 File Download

Scenario

When an end user downloads a file, a progress message box is displayed. The file is downloaded from the Internet to the Threat Isolation Gateway. The message box displays the progress of the file download as a percentage.



After the file is downloaded to the Gateway, the progress message box displays the file sanitizer scanning of the downloaded file.

8.2.1 Download Profiles

Download Profiles are set up to specify the action Symantec Threat Isolation should take, depending on the file type or the category of the file to be downloaded. For more information about defining Download Profiles, see section [4.3.4 "Defining Download Profiles"](#).

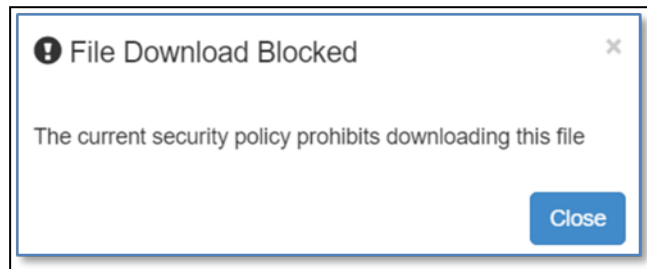
8.2.1.1 Profile Setting: Allow

When the Download Profile setting is Allow, the file is downloaded and considered safe.



8.2.1.2 Profile Setting: Block

When the Download Profile setting is Block, the file is blocked and a message is displayed, stating that the current security policy prohibits downloading this file. The block action for this file type is initiated before the file sanitizer scan.

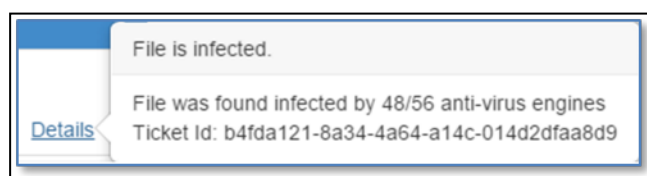


8.2.1.3 Profile Setting: Scan

When the Download Profile setting is Scan, the file to be downloaded is scanned. If a virus is found, a warning message is displayed, stating that the file is infected and cannot be downloaded.

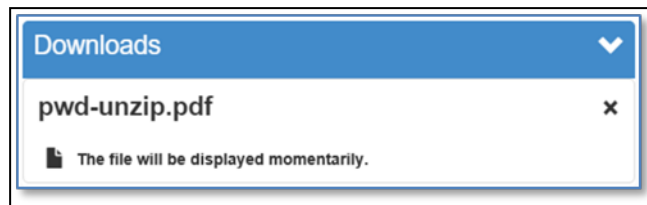


Clicking Details displays a tracking ticket number and any additional file sanitizer results. The tracking ticket number can be searched in the activity logs.



8.2.1.4 Profile Setting: View

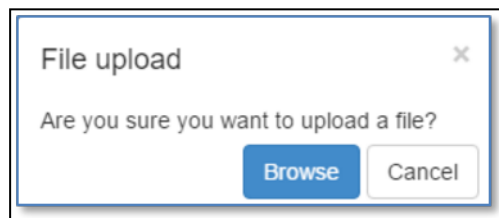
When the Download Profile setting is View, the user will not be able to download files, but only view them in a secure document isolation environment. For more information about the document isolation environment, see section [4.3.3.1 "Overview"](#). In the case of extremely large files, the following message might be displayed.



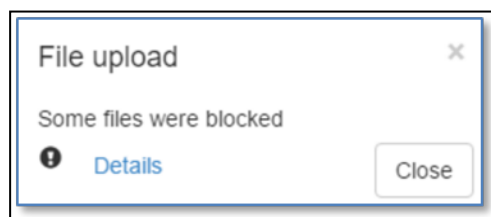
8.3 File Upload

Scenario

When an end user uploads a file, a pop-up window is displayed. The window verifies that the user intended to upload a file, and the end user should click Browse to select the file for uploading.



If the upload profile blocks the uploading of files or file types, an error message is displayed, advising the end user that the upload is blocked. If multiple files are uploaded and some but not all of the file types are blocked, the error message states that Some files were blocked. The user is prompted to click Details to view the list of blocked files.



Reason

Uploading files or the movement of data poses a security concern.

More Information

For more information about uploading files and upload profiles, see section [4.3.5 "Defining Upload Profiles"](#).

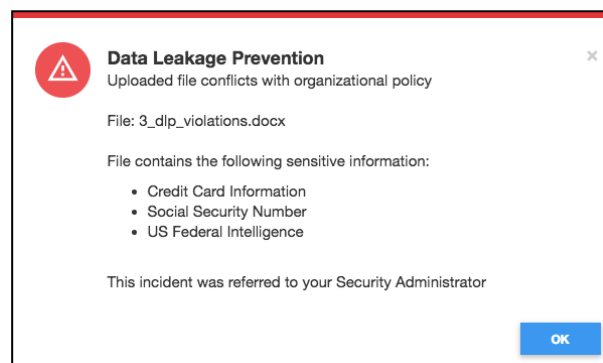


8.4 Data Leakage Prevention

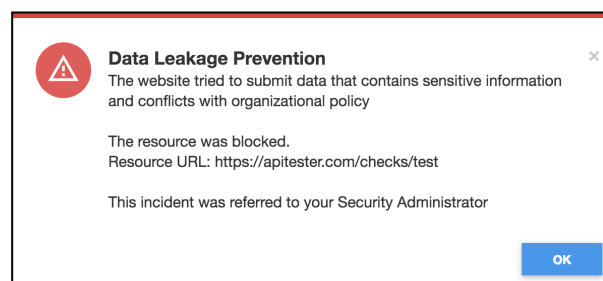
Scenario

When an end user uploads a file, a Data Leakage Prevention pop-up window is displayed.

- The window shown below is displayed when the file that the end user tried to upload was blocked by Data Leakage Prevention (DLP). The window specifies each DLP violation found in the file.



- The window shown below is displayed when the end user initiates a network request with body data that is blocked by DLP.



Reason

This mechanism prevents sensitive data, such as credit card information and Social Security numbers, from being leaked to entities outside the organization.

More Information

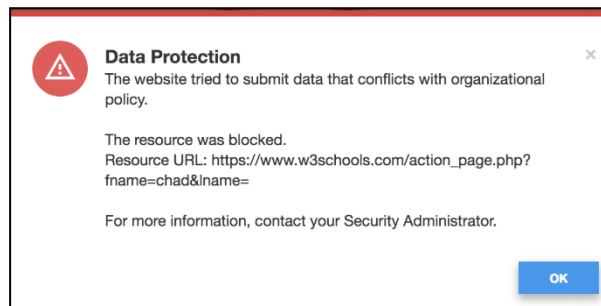
For more information about DLP, see sections [4.18 "Configuring Data Leakage Prevention Server Settings"](#) and [4.18.1 "Adding Data Leakage Prevention Server Settings"](#).



8.5 Data Protection

Scenario

When an end user uploads a file, a Data Protection pop-up windows is displayed, as shown below.



Reason

This window is displayed when a top-level navigation resource and/or a subresource was blocked because data criteria were matched in the body or the query parameters. This means that the data was found to contain sensitive information that conflicts with your organizational policy.

More Information

For more information, see sections [4.4.9.3 "Creating Data Criteria"](#) and [4.4.9 "Creating Request Filters"](#)

8.6 Block Page

Scenario

When a policy rule is setup to block a website, the end user sees a screen message stating that the website is blocked based on company policy. The Management user can customize this message.

Reason

Many companies block websites that have known security concerns or are not related to company business directives.

More Information

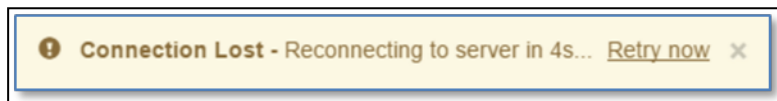
To add or update block pages, see section [4.4.6 "Creating Custom Pages"](#).



8.7 High Availability Failover

Scenario

To maintain constant network access to a Threat Isolation Engine (TIE), an automatic failover mechanism is established. If the current TIE is no longer available and a new connection to a different TIE must be established, the message Reconnecting to server in X seconds is displayed.



Reason

Network connectivity to the TIE is necessary to ensure that the highest security protocols are in place.

More Information

- See section [5.2.3.4 "Failover"](#).
- High Availability and Load Balancing are explained in detail in chapter [5 "High Availability and Load Balancing"](#).

8.8 Pause Functionality

Scenario

When a continuous movement, such as a stock ticker or active advertisement is shown on the browser and there is no user interaction with the keyboard or mouse for 60 seconds, the continuous movement is paused. A pause symbol is displayed on the bottom right of the screen. The movement can be reinstated by pressing any key on the keyboard or moving the mouse.



Reason

This occurs to save bandwidth between the end user and the Threat Isolation Engine (TIE) due to continuous rendering of the data while the user is not interacting with browser.

More Information

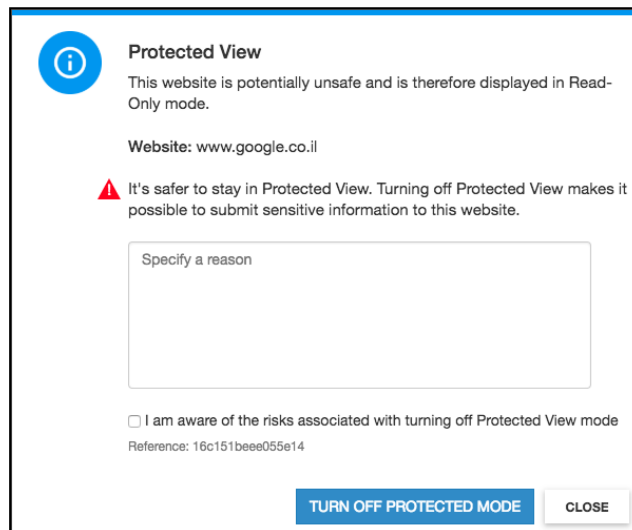
See section [4.4.10.2 "Idle Mode Setting"](#).



8.9 Read-Only Webpages

Scenario

When an end user browses to a specific website, the website is rendered in read-only mode (meaning that all of its input fields are disabled) and a message is displayed.



Reason

This occurs when a user browses to a website that is potentially unsafe. Read-only mode prevents the user from submitting sensitive information to this website.

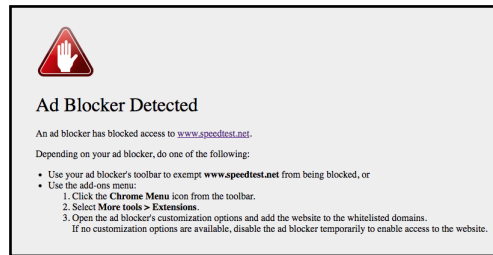
More Information

For information about disabling all input fields when a website might be unsafe, see section [4.3.7.2 "Adding an End-User Data Protection Profile"](#).

8.10 Ad Blocker

Scenario

The end user experiences connectivity issues, and the following message is displayed in the browser: "Ad Blocker Detected".



Reason

This occurs when Symantec Threat Isolation's ad blocker detection capability is enabled and has detected an ad blocker that is blocking access to the requested website.

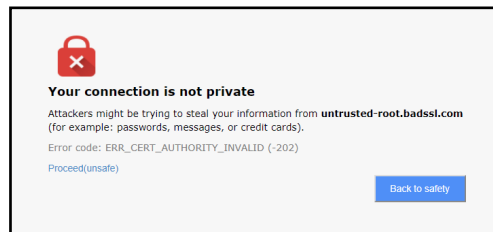
More Information

Ad blocker detection is disabled by default. For information about enabling this capability, see section [9.3.1.12 "Ad Blocker Detected"](#).

8.11 Untrusted Certificate

Scenario

The following message is displayed in the endpoint browser: "Your connection is not private".



Reason

This occurs when the end user tries to visit a website with a server certificate that the Threat Isolation Engine (TIE) does not trust. The TIE warns the user that proceeding to the website is unsafe.

More Information

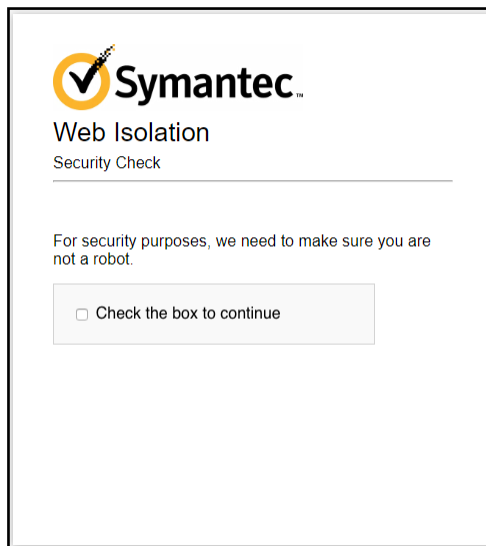
For information about adding customized text to this message, see section [4.9.5 "Adding Customized Text to the Untrusted Certificate Message"](#).



8.12 Anti-Bot Captive Page

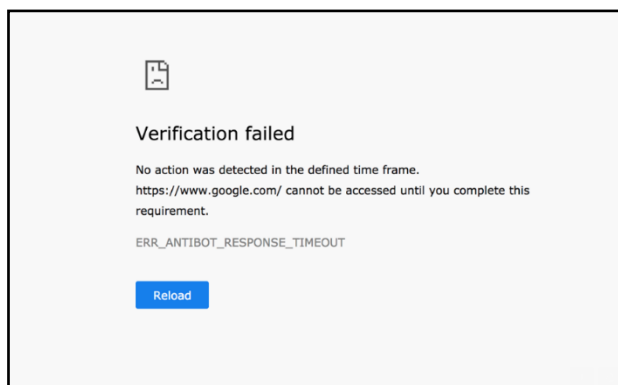
Scenario

The following page is displayed in the endpoint browser:



Reason

This occurs when a new browser or tab is opened where an Anti-Bot Protection Profile applies. The end user needs to get past the anti-bot captive page before they can access the requested page. If no response is received within the configured timeout period, the following is displayed:



More Information

For information about Anti-Bot Protection Profiles, see section [4.3.9 "Defining Anti-Bot Protection Profiles"](#).



8.13 Document Isolation Viewer: Linked File Opens in Same Tab

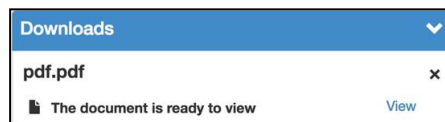
Scenario

When the end user browses a webpage and clicks on a link to a document with a View action, that document is viewed using the Document Isolation Viewer and opens in the same tab, on top of the webpage that contained the link.

Reason

This is the default action (by default, the Download Profiles advanced setting `viewDocumentInNewTab` is set to `False`).

If `viewDocumentInNewTab` is set to `True`, the following pop-up message will appear when the end user clicks on the link:



When the user clicks View, the document opens in a new tab and is viewed using the Document Isolation Viewer.

More Information

For information about the advanced setting `viewDocumentInNewTab`, see the section ["Configuring Symantec Cynic Scanning Mode for a Download Profile"](#).



9 Troubleshooting

9.1 Tools

Symantec Threat Isolation provides various tools to help you troubleshoot common issues.

9.1.1 Activity Logs

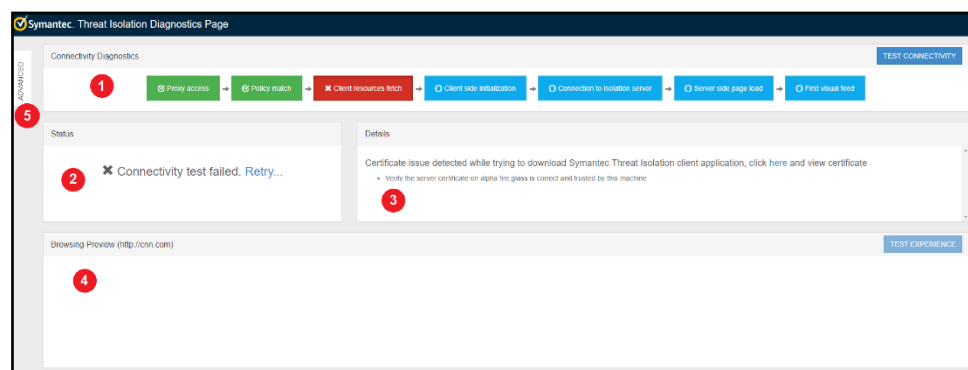
In addition to detailed network logs (and Session view), the activity logs include specific logs that can be of use in troubleshooting any issues. For example, an application failed to authenticate, a page failed to load, and so on.

The activity logs enable you to view activity logs of the user who experienced the issue and find the resource that caused it. You can then find the relevant rule to understand why the issue occurred. For more information, see section [6.1 "Activity Logs and Analytics"](#)

9.1.2 FGDiag

The FGDiag diagnostic tool resides on the end-user side and assists you in troubleshooting website connectivity and client-to-proxy and Threat Isolation Engine (TIE) connectivity issues. To display the tool, the end user should add the following suffix to the website URL: **/fgdiag**. For example, <https://www.cnn.com> would appear as <https://www.cnn.com/fgdiag>.

FGDiag performs connectivity testing automatically, and detects and indicates the failing component. In case of a slowness issue, the end user can generate a report with diagnostic information by clicking Test Experience, and send the text file to the Management user for further handling.





The FGDiag window, shown in the figure above, consists of the areas listed in the following table. The number for each area in the table corresponds to the same number in the figure.

	Area	Description
1	Connectivity Diagnostics	Represents the diagnostic steps flow
2	Status	Displays the status of the connectivity test
3	Details	Provides details of the test results and suggestions for solving the detected connectivity issue
4	Browsing Preview	Displays a preview of the browsed webpage
5	Advanced	<p>Provides diagnostic information about the Resource Server and the Application Server:</p> <ul style="list-style-type: none">■ Resource Server - The Threat Isolation Gateway where sub-resources needed for communication with the isolation server are downloaded. This can be any Gateway machine■ Application Server - The Gateway where isolation is done. This is always a TIE machine

The Connectivity Diagnostics area in the FGDiag window represents the flow of the diagnostic stations, explained in the following table. The diagnostic station where an issue is found, appears red.

Step	Description
Proxy access	Checks the connection to the proxy server and scans for proxy settings issues
Policy match	Detects policy-based issues
Client resources fetch	Detects issues with downloading the sub-resources needed to communicate with the isolation server
Client-side initialization	Detects issues indicating a failure in client-side initialization
Connection to isolation server	Detects WebSocket and DNS issues
Server-side page load	Detects issues that prevent the server-side browser from loading the page
First visual feed	Detects issues that occurred while loading the visual stream to the endpoint



The Advanced section of the FGDiag page provides diagnostic information about the Resource Server and the Application Server, which is useful in determining in which Gateway and component the failure occurred.

9.1.2.1 Table of Common Connectivity Issues

The table below lists the messages that appear when common connectivity issues occur between the endpoint browser and the Threat Isolation Gateway, and provides troubleshooting suggestions for each issue.

Studying this table will give you a better overall understanding of the system flows, the possible issues and their solutions before you ask the end user to run fgdiag in their browser. The fgdiag diagnostic tool automatically detects connectivity errors on the endpoint machine, and displays the relevant error message and troubleshooting suggestions in the endpoint browser according to the use case in their environment.

Message	Suggestions	See section
No connectivity to the proxy server	<ul style="list-style-type: none">■ Restart your browser to make sure it uses the latest PAC script version:<ul style="list-style-type: none">◆ Navigate to <code>http://<Threat Isolation Proxy Public DNS Name>:8081/proxy.pac</code> and verify that your browser has downloaded the PAC script successfully■ If you are using a browser extension for your PAC script configuration, replace it with the system proxy configuration■ If you are using Symantec Threat Isolation as a proxy:<ul style="list-style-type: none">◆ Make sure you have access to your proxy on port 8080◆ Check services health on <Resource Server> by running 'fgcli service status'	3.6.1 "Configuring the Symantec Threat Isolation Explicit Proxy Topology"
Authentication error, unable to authenticate this client	<ul style="list-style-type: none">■ Verify your Active Directory or internal user configuration■ For Kerberos authentication, verify your Keytab file	<ul style="list-style-type: none">■ 4.5.1.1 "Creating Internal Users"■ 4.5.2 "Defining Active Directory Settings"■ 4.5.3 "Creating Keytab Settings"



Message	Suggestions	See section
Certificate issue detected, click <here> and view certificate	<ul style="list-style-type: none">■ Make sure the browser trusts the root CA certificate■ Make sure the root CA certificate configured on your proxy server is correct	<ul style="list-style-type: none">■ 3.5.11 "Installing the CA Certificate as Trusted Root CA on the Client Side"■ 3.5.12 "Verifying the Trusted Root CA in the Endpoint Browser"
You've tried to navigate to an HTTPS site when Symantec Threat Isolation system is configured to work in HTTP only mode	<ul style="list-style-type: none">■ If HTTPS site isolation is required, login to Symantec Threat Isolation Management Admin and set System Configuration>Advanced Configuration> httpOnly.useSsl to true	3.5.7 "Defining the Management Gateway"
Unable to download Symantec Threat Isolation client application from <Resource Server>	<ul style="list-style-type: none">■ Make sure your system firewall rules are configured to allow traffic on ports 80 or 443 to <Resource Server>■ Check services health on RESOURCE_SERVER_PARAM by running 'sudo fgcli service status'	



Message	Suggestions	See section
No HTTP connectivity to <Resource Server>	This issue indicates a misconfiguration between the PAC file isolation server rule and the HTTP server configuration on <Resource Server>. Contact Symantec Threat Isolation technical support for further investigation	3.6.1.1 "Editing the Proxy Auto-Configuration (PAC) File" When you have made your changes, close the Update Threat Isolation Engine Affinity window
No WebSocket connectivity to <Application Server>	This issue can be caused by one of the following: <ul style="list-style-type: none">■ The Application Server DNS entry was not configured with a proper wildcard entry: *.<Application Server> must point to <Application Server>. NOTE: Make sure the DNS supports wildcards■ Ad Blocker or another browser extension is blocking the WebSocket connection on this website. NOTE: When ad blocker detection is enabled, Symantec Threat Isolation will detect ad blockers automatically	<ul style="list-style-type: none">■ 3.4.3 "Defining Networking"■ 8.10 "Ad Blocker"
Isolation server <Application Server> is probably down	This issue can be caused by a failure to establish a TCP connection between the client and the <Application Server> on port 443 or 80. For further analysis, run 'sudo fgcli service status' on <Application Server>. Contact Symantec Threat Isolation technical support for further investigation	
You are using an ad blocker	Your ad blocker is blocking access to some paths of <Destination URL host> and to other domains, including the Symantec Threat Isolation server. Configure your ad blocker to allow ads on <Destination URL host>. If no customization options are available, disable the ad blocker temporarily to enable access to the website. NOTE: When ad blocker detection is enabled, Symantec Threat Isolation will detect ad blockers automatically	8.10 "Ad Blocker"



9.1.3 fgcli

All Symantec Threat Isolation CLI functionality is invoked using fgcli. Run the relevant fgcli command(s) and handle the output, or send the output to Symantec Threat Isolation technical support for further handling. Note that some diagnostics are optional; they might be disabled when the configuration does not need them.

9.1.3.1 Diagnostic Commands

Threat Isolation Gateway diagnostic commands perform various types of system diagnostics, such as network tests and basic components sanity diagnostics.

Command	Description
fgcli diagnostics [-v]	Runs all system diagnostics
fgcli diagnostics -t <diagnostic-path> [-v]	Runs a specific diagnostic test

If no issues are detected, the diagnostic tool will report the system status “OK” (green). In case of system failure, diagnostic failure results are formatted as follows:

	Description
Status	System status: warning (yellow), or failed (red)
Description	Explanation of the diagnostic
Issue	Title of the error message
Error messages	Contents of the error message
Remedies	Instructions for solving the issue

To run a specific diagnostic (for example, the diagnostic that failed):

1. Run the following command:

```
fgcli diagnostics -t
```
2. Double-click tab to display all available test names.
3. Type the name of the required test:

```
fgcli diagnostics -t [test name]
```
4. Press Enter.

9.1.3.2 Statistics Commands

Statistics commands provide more comprehensive user and system-related information. Unlike activity logs, which are useful for analyzing network or HTTP-related issues that occurred in the past (see section [9.1.1 "Activity Logs"](#)), fgcli



statistics commands enable you to gather system information about the tabs that are currently open. For example, you can use fgcli statistics commands to find the IDs of the tabs that consume the most CPU, and then close these tabs using the fgcli kill-tabs command.

Command	Description
fgcli stats all	Prints all tab statistics in JSON format
fgcli stats all --sort-by memory_usage	Gets all tabs sorted by memory usage
fgcli stats all --sort-by user_name grep user_name uniq --count sort -n	Gets the number of tabs per user
fgcli stats where user_name eq john --sort-by creation_time	Gets all of John's tabs, sorted by creation time
fgcli stats where active_downloads gt 0	Gets all tabs with active downloads
fgcli stats where active_last_requested_url match ".symantec.com.*" --sort-by memory_usage	Gets all open symantec.com tabs, sorted by memory usage

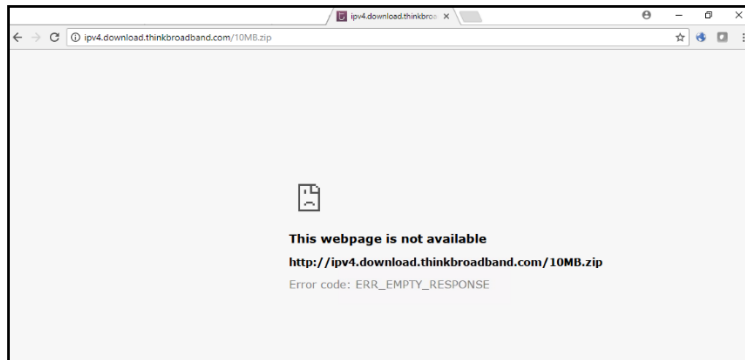
9.1.3.3 Miscellaneous fgcli Commands

The following fgcli commands enable you to perform general tasks.

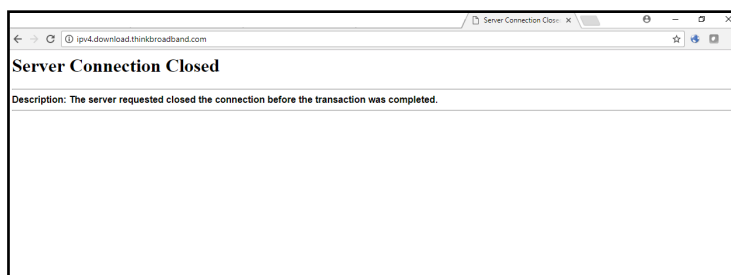
Command	Description
fgcli system ipv6 enable	Enables IPv6 addresses in Threat Isolation Gateway network interfaces
fgcli system ipv6 disable	Disables IPv6 addresses in Threat Isolation Gateway network interfaces

9.2 Error Message Format

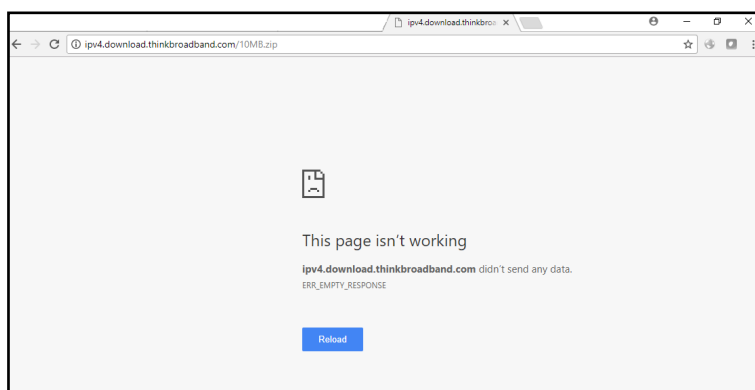
Error messages that indicate Threat Isolation Engine (TIE), Threat Isolation Proxy, or client-side issues each have a distinctive look and feel. The different error message formats enable you to see at a glance to which component the issue you are troubleshooting relates.



Note that in TIE error messages, the context menu is the isolation context menu.



Note that in client-side error messages, the context menu is the native context menu.





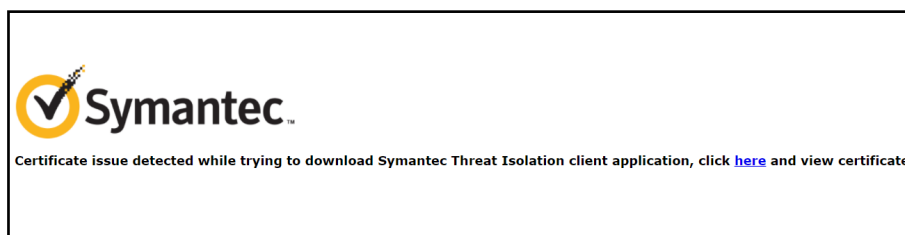
9.3 Common Issues

9.3.1 Client Side

9.3.1.1 CA Certificate Not Trusted

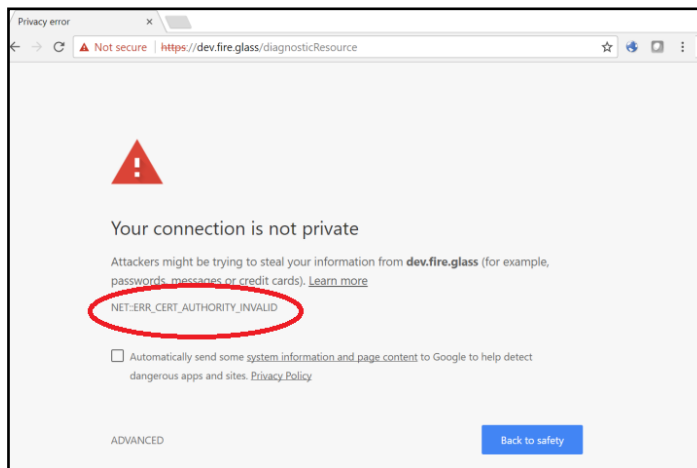
User Experience

A blank page appears, and after approximately 30 seconds the following message displays, regardless of the website to which the end user has browsed:



Solution

When the end user clicks the link to view the certificate, the following message is displayed:



The end user should click the error (marked in red in the figure) specified in the message. If the following information is displayed, the endpoint browser does not trust the Zone CA:

Subject: <Gateway host name>

Issuer: <Zone CA certificate>



To solve the issue, add the CA to the list of trusted certificates (see section [3.5.11 "Installing the CA Certificate as Trusted Root CA on the Client Side"](#)).

Note

Internet Explorer and Chrome consult with the operating system's CA store, which can be deployed remotely via the Windows infrastructure. Firefox, on the other hand, maintains its own CA store. If the solution given above solved the issue for Internet Explorer and Chrome, but not for Firefox, refer to section [3.5.11.3 "Installing the CA Certificate in a Firefox Browser"](#) for more information.

9.3.1.2 Internet Explorer Does Not Show Isolated Page; Chrome Does

User Experience

Internet Explorer (IE) users see a blank page, while Chrome users see the isolated webpage.

Solution

This issue is usually related to an IE security feature. Make sure the instructions given in section [3.4.3.1 "TIE Public DNS Name Considerations"](#) have been implemented. If the issue still occurs, you have the following options:

- If you cannot assign a domain name to your Threat Isolation Engine (TIE) Gateways that is different than your organization's domain name, configure IE explicitly to consider the TIEs to be in the Internet zone.

For more information, see the following links:

- ◆ <https://support.microsoft.com/en-us/help/174360/how-to-use-security-zones-in-internet-explorer>, and
 - ◆ <https://support.microsoft.com/en-us/help/303650/intranet-site-is-identified-as-an-internet-site-when-you-use-an-fqdn-o>.
- (Less recommended) If the client-side environment and TIE servers are in the same Intranet zone, customize the IE default settings for that zone.

Go to Internet Options > Security tab > Local intranet > Sites and clear both of the following checkboxes:

- ◆ Include all local (Intranet) sites not listed in other zones
- ◆ Include all sites that bypass the proxy server



9.3.1.3 Access to Any Isolated Webpage Is Blocked

Experience

End users cannot access any isolated webpage.

- In the Chrome browser, the following error message is displayed.



- In the Firefox or Internet Explorer (IE) browser, the following error message is displayed.



Background

These messages indicate that the Threat Isolation virtual shared domain could not be reached due to client-side browser configuration.

- In the Chrome browser, the issue occurs when access to third-party cookies is blocked. The Symantec Threat Isolation block page, contains client-side logic for initiating a WebSocket directed to the Threat Isolation Engine (TIE). The block page loads a hidden iframe that tries to access the virtual shared domain used by Symantec Threat Isolation for storing persistent client configuration and preferences. The virtual shared domain is therefore required to achieve isolation. However, since Symantec Threat Isolation uses a hidden iframe to load the shared domain, endpoint browsers might mistakenly detect it as a third-party cookie (tracker) and block it. As a result, website isolation will fail.
- In Firefox and Internet Explorer browsers, the issue occurs when local storage is disabled in the endpoint browser. Symantec Threat Isolation uses the local storage of its virtual shared domain, <https://global-shared.fire.glass>, to maintain contextual information persistently. If access to local storage is disabled, the shared domain will not work and website isolation will fail.



Solution

Chrome

1. At the top right, click More and then Settings.
2. Click Advanced.
3. Under Privacy and Security, click Content Settings.
4. Make sure the Block third-party cookies and site data checkbox is clear.

Firefox

1. In the address bar, type about:config and press Enter.
2. Click I accept the risk!
3. In the about:config page, search for the dom.storage.enabled entry. The default value for this entry is "true". If the listed value is "false", double-click dom.storage.enabled to change the value to "true".

Internet Explorer (IE)

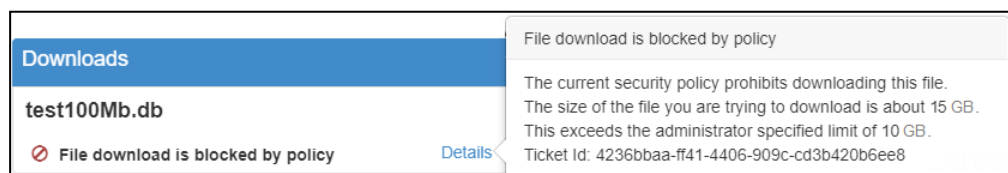
1. From the Tools menu, choose Internet Options.
2. Display the Advanced tab.
3. Under Settings, scroll down to the Security section.
4. Check Enable DOM Storage and click OK.
5. In the %userprofile%\Appdata\LocalLow directory, make sure the integrity level is set to Low. This allows non-administrator users to write data to local storage. Use the following command:

```
icaccls %userprofile%\Appdata\LocalLow /t /setintegritylevel  
(OI) (CI) L
```

9.3.1.4 Downloading A Bigger File Than Permitted by Policy

User Experience

The end user sees a Downloads error message where the details explain that the file download was blocked by policy, because it exceeded the maximum file size.





Solution

As a Management user, take the Ticket Id provided in the details of the Downloads error message and enter it into the activity log. (Note that the end user should copy the Ticket Id and send it to the Management user.) This enables you to view the matched rule according to which the download was blocked and check its Downloads Profile (for more information, see section [4.3.4.4 "Adding a Download Profile"](#)).

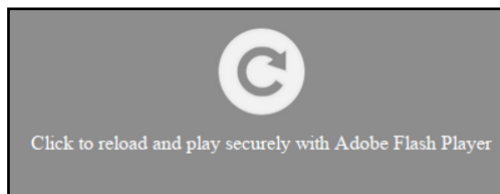
You have the following options:

- In the matched rule, extend the maximum size of the Downloads Profile (for more information, see section [4.3.4.4 "Adding a Download Profile"](#), Max Download Size).
- Create a custom rule for specific users who need to download bigger files, with a greater download size limitation.
- Tell the end user they are not allowed to download a file of this size.

9.3.1.5 Flash Video Not Displayed

User Experience

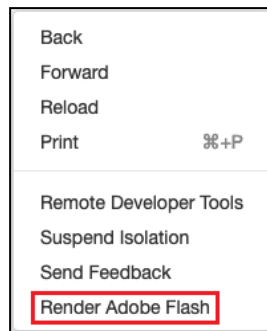
On rare occasions, when a webpage runs a Flash video, end users might see a message asking them to click the screen to play the video securely.



Solution

Symantec Threat Isolation enables end users to watch Flash video securely by playing Flash media on the Threat Isolation Engine (TIE) and not on the local machine, thus adding an extra layer of protection (for more information, see section [8.1.4 "Render Adobe Flash"](#)).

However, when users browse a website that uses a lot of Flash media, they might be asked to select Render Adobe Flash from the context menu. This enables the Adobe Flash plug-in, and the Flash video is loaded on the current website's hostname and tab within the browser. This ad hoc solution does not affect the sessions of other users.



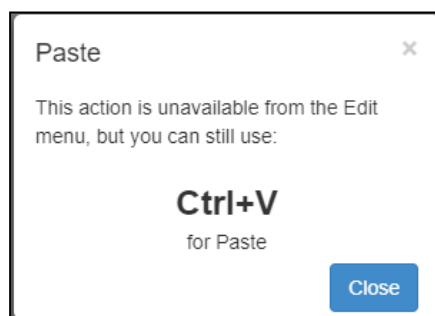
As a Management user, report this issue to Symantec technical support so the user will not experience the issue repeatedly.

The Render Adobe Flash option can also be displayed from the Advanced Options screen. Note that this option is available only when Symantec Threat Isolation does not enable Flash rendering automatically in the browsed website. For more information, see section [4.3.3.2 "Adding an Isolation Profile"](#).

9.3.1.6 Paste Nonfunctional from the Custom Symantec Context Menu

User Experience

If the custom Symantec context menu is enabled, when the end user right-clicks in a text area of an isolated webpage, the Cut, Copy and Paste options are displayed. Cut and Copy can be performed. However, when the user chooses Paste, the following message appears:



Solution

The keyboard keys Ctrl+V can be used to paste cut or copied text.

9.3.1.7 Isolated Websites Look Different Than Non-Isolated Ones

User Experience

The end user observes that an isolated webpage they browsed to looks different than the same webpage without isolation.



Solution

Symantec Threat Isolation runs a Linux Chromium browser on the server side. In some cases, rendering differences might occur between operating systems.

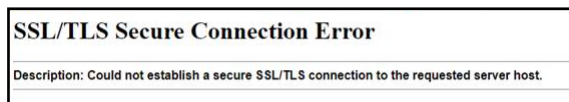
If your organization has Linux users, ask them to open the webpage on their Linux machine and see if the isolated webpage behaves the same way as the Linux-bypassed webpage. If it does, then this is the isolation experience.

For organizations that do not have Linux users, Symantec Threat Isolation provides a cloud-based Linux machine, Apache Guacamole™, on which to test the issue. For more information, contact Symantec Threat Isolation technical support.

9.3.1.8 SSL/TLS Secure Connection Error

User Experience

When the end user visits an inspected site, an SSL/TLS Secure Connection error message is displayed: The Threat Isolation Proxy could not establish a secure SSL/TLS connection to the requested server host.



Solution

The template of this SSL/TSL error message indicates that the Threat Isolation Proxy failed to create a secure tunnel with the next hop proxy/server (for more information, see section [9.2 "Error Message Format"](#)).

- If only a specific HTTP website experiences the issue, the certificate of this website is not trusted. You have the following options:
 - ◆ (Recommended) Add the server certificate of the specific website to the list of Trusted Certificates (see section [4.9.3 "Adding a Trusted Certificate"](#)).
 - ◆ (Less recommended) Add a rule to your policy to bypass this specific website. This option is recommended only if the first option did not solve the issue. If you solve the issue using this option, contact Symantec Threat Isolation technical support. **Important:** Once the support ticket is resolved, remove the bypass rule.



- ◆ (Not recommended) Add a temporary exclusion code in the Proxy Auto-Configuration (PAC) file, instructing the browser to go to this website directly and not via the Threat Isolation Proxy. It is not recommended, since bypassing the Proxy means there will be no activity logs. If you solve the issue using this option, contact Symantec Threat Isolation technical support. Note that this option requires you to adjust your firewall rules to allow connectivity to the Internet from the specific machine. **Important:** Once the support ticket is resolved, remove the exclusion code from the PAC file.
- If all websites experience the problem, it indicates a next hop proxy/server SSL interception issue. Do the following:
 - ◆ Add the CA certificate of the next hop proxy/server to the list of Trusted Certificates.

9.3.1.9 Incorrect URL Categorization

User Experience

The end user sees a block page, stating a reason for the blocking that seems to be unrelated to this webpage.

Solution

This issue might point to incorrect URL categorization, or misclassification. When the end user reports a misclassification, do the following:

1. Reproduce the issue by browsing to the same website.
2. In the activity log, enter the Ticket Id in the Tab Id field.
3. Under Categories, find the rule responsible for blocking the webpage.
4. Follow the URL to [GIN](#), the URL categorization vendor that Symantec Threat Isolation uses, and type the URL of the misclassified website.
5. If the website is misclassified, contact Symantec Threat Isolation technical support.

Notes

- If all URLs are uncategorized, make sure the Threat Isolation Proxy has connectivity to the Internet, or check the Firewall Rules table (see the Defining Firewall Rules section relevant to your deployment topology).
- If your organization's policy does not allow Threat Isolation Proxy connectivity to the Internet, then it is recommended not to use URL categorization.



9.3.1.10 Slowness Issues

User Experience

The end user complains of system slowness.

Solution

The causes of slowness might be difficult to identify, because there can be many different factors at play, such as:

- High CPU
- High memory
- Latency
- Bandwidth
- Other Threat Isolation Gateway performance issues, such as I/O
- Disk space

Before turning to Symantec Threat Isolation technical support, you can help shorten the troubleshooting process by doing the following:

1. Display the Gateways page and see if any Gateway has high-usage issues. For more information, see section [4.7.5 "Understanding the Gateway Settings Table"](#).
2. Once you have pinpointed the relevant Gateway, consider the following possibilities:
 - ◆ There might be a load-balancing issue
 - ◆ The Gateway might be overloaded. In this case, find out which tabs are causing the problem (for example, using `fgcli stats`) and then kill them using the `fgcli kill-tabs` command.
 - ◆ If your tabs are killed automatically and the browser is black or gray, check your spec and compare it to the Symantec Threat Isolation sizing guide to see if there is enough memory for the number of users
 - ◆ There might be a latency issue. In this case, use the `FGDiag` tool and send a report to Symantec Threat Isolation technical support

9.3.1.11 Proxy.PAC File Not Accessible

User Experience

A blank page displays, no matter which website the end user visits.



Solution

This issue indicates that the Threat Isolation Proxy is always bypassed. Try the following:

- Make sure you have performed every step described in section [3.6.1 "Configuring the Symantec Threat Isolation Explicit Proxy Topology"](#).
- In the Proxy settings, verify that you have defined the Proxy on your browser. For more information, see section [3.6.1.3 "Verifying PAC File Configuration in the Endpoint Browser"](#).
- A connectivity issue might exist between the client and the Proxy even though the Proxy is configured properly. For example, port 8081 - the port through which the Proxy Auto-Configuration (PAC) file is downloaded - might not be opened globally, causing new end users or end users on a new machine to experience isolation issues.

Download the PAC file manually from the end user browser by opening the following URL: `http://<proxy public DNS name>:8081/proxy.pac`.

If the proxy.pac is not downloaded, verify that port 8081 was opened globally.

If the proxy.pac is downloaded, do the following in Chrome:

- ◆ Open the URL <chrome://net-internals/#proxy> and make sure the Threat Isolation Proxy is defined in the effective proxy settings.
- ◆ Open the URL <chrome://net-internals/event> and filter by PAC. Look for records displayed in red, and debug the issue using the information contained in them.

For assistance, contact Symantec Threat Isolation technical support.

9.3.1.12 Ad Blocker Detected

User Experience

A blank page is displayed in the endpoint browser.

Solution

This might occur because an ad blocker is installed on the endpoint machine.

When ad blocker detection is enabled on the endpoint browser, Symantec Threat Isolation detects that an ad blocker is blocking access to the website the end user is trying to visit, and displays the message "Ad Blocker Detected" in the endpoint browser. For more information, see section [8.10 "Ad Blocker"](#).

By default, ad blocker detection is disabled. In this case, a blank page is displayed in the endpoint browser.

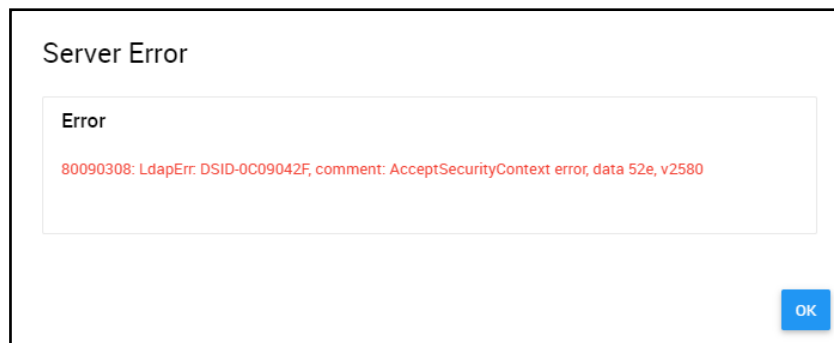


1. To enable ad blocker detection, go to:
Policy Advanced Settings > Internal Settings
For more information, see section [4.4.11 "Creating Policy Advanced Settings"](#).
2. Enable the parameter `proxy.adblock_detection_enabled`.

9.3.2 Management Side

9.3.2.1 Active Directory Settings Server Error

When bad credentials are provided, a Server Error message appears in the Active Directory Settings > Active Directory Configuration. The error message below signifies a bad username or password.



This error message might appear even when the password is correct, but a bad username format is used. Some organizations use a different username format, such as `<domain>\<user>`, `<user>@<domain>`, and so on. Note that the provided username must conform to the format that is used in Active Directory (AD).

9.3.2.2 Push Settings

Pushing settings might fail. Troubleshooting this issue depends on whether the Threat Isolation Gateway is newly created or has an existing policy:

- If the Gateway is new, make sure ports 3004 and 3005 are open from the Gateway to the PDP. For more information, see the Defining Firewall Rules section relevant to your deployment topology and the descriptions of ports 3004 and 3005 in the table.
- If the Gateway has an existing policy, copy the error text and contact Symantec Threat Isolation technical support.



In both cases, if the issue persists, run the following command on the Gateway where pushing settings failed:

```
fgcli diagnostics
```

and send the output to Symantec Threat Isolation technical support.

9.3.2.3 Licensing

Online Registration Failure

When registering the license online, the following error message might appear under Serial Number: “No network access to licensing service (host: licensing.services.fire.glass)”. This occurs when there is no network access from the endpoint that runs the Management web UI to licensing.services.fire.glass.

Solution:

- Make sure the endpoint that runs the Management web UI has network access to licensing.services.fire.glass.
- If the above cannot be done, register the license offline. For more information, see section [4.20.1.2 "Registration"](#).

Online Update Failure

The following error message might appear in the Create License Settings dialog, under License Information: “Runtime exception. Could not verify and prepare httpOptions StackTrace”.

Create License Settings

License File ?

[Hide Information...](#)

License Information

Push settings to apply information on gateways

Serial Number 1002650022

Runtime exception. Could not verify and prepare httpOptions StackTrace.

Last updated 3 minutes ago

Name	Activation Date	Expiration Date	Product Description
Anti-Phishing	2017-11-20	2019-12-31	Full Web Isolation Virtual Appliance Linux, License, 1-99 Users
Document Isolation	2017-11-20	2019-12-31	Full Web Isolation Virtual Appliance Linux, License, 1-99 Users



This occurs when Internet access is disabled for the Threat Isolation Gateway, or when there is no access to `licensing.services.fire.glass`.

Solution:

- Make sure that at least one Gateway has Internet access (for more information, see section [4.7.7 "Defining a Threat Isolation Gateway"](#)). Even if a Gateway has no direct Internet access, it can still access the Internet via another Gateway that communicates with the same PDP.
- Allow the Gateways that have Internet access to access `licensing.services.fire.glass` from host of the web UI client. How this is done, depends on your topology.
- If the above cannot be done, register the license offline.

Rule Warning

An error text similar to the following one might appear in the rules table in the Policy page: “Your license does not entitle you to use Risk Level destination(s)”. This occurs when there is no license for the required subscription.

	Active	Client Ap...	User	Source	Destinati...	Action	Downloa...	Logging	Description	Updated At
Applications...	<input checked="" type="checkbox"/>	Any	Any	Any	Product... File St... Collab... Person... Instant... Brows...	Pass		Prima...	(System ...	5 months ago
Rule	<input checked="" type="checkbox"/>	Any	Any	Any	Any	Block		Prima...		a minute ago
Rule	<input checked="" type="checkbox"/>	Browsers	Any	Any	Any	Block		Prima...	Default R...	7 months ago
Rule for Ap...	<input checked="" type="checkbox"/>	Applicatic	Any	Any	Any	Pass		Prima...	Default R...	7 months ago

Solution:

- Make sure the license includes the required subscription.
- Push settings when the license is registered or updated.

Categorization Failure

The following error text might appear in the Details column of the activity log table: “Failed to access Symantec Global Intelligence Network”. This occurs when there is no access to Symantec Global Intelligence Network (GIN) services, or when no valid license exists.

Resource One	Resource Two	Destination IP	Host	Port	Host Name	Resource One	Details
bat.bing.com/action/...		204.79.197.200			Default R...	edition.cnn...	Failed to access Symantec Global Intelligence Netw
cdn3.optimizely.com...		23.44.249.173			Default R...	edition.cnn...	Failed to access Symantec Global Intelligence Netw
sharethrough.adnxs...		37.252.172.27			Default R...	edition.cnn...	Failed to access Symantec Global Intelligence Netw
a125375509.cdn.opti...		92.122.13.82			Default R...	edition.cnn...	Failed to access Symantec Global Intelligence Netw



Solution:

- Check the installed license and its subscriptions.
- Make sure network access to GIN services exists:
`webpulse.es.bluecoat.com`
`subscription.es.bluecoat.com`

9.3.3 Threat Isolation Gateway Side

9.3.3.1 Upgrade Failure

The Symantec Threat Isolation system upgrade procedure (for more information, see section [3.9 "Upgrading the Symantec Threat Isolation System"](#)) might fail due to insufficient disk space. The following message appears: "No space left on device".

It is recommended to make sure sufficient disk space is available on your machine before starting the upgrade:

1. Run the following Linux command to display the amount of disk space available on your machine, per partition:

```
df -h
```

For example, the output of the above command could be:

Filesystem	Size	Used	Avail	Use%	Mounted on
Udev	16G	4.0K	16G	1%	/dev
Tmpfs	3.2G	6.7M	3.2G	1%	/run
/dev/dm-0	110G	12G	93G	12%	/
/dev/mapper/system-var	123G	111G	12G	90%	/var
/dev/loop0	46G	53M	44G	1%	/var/fireglass/downloads
/dev/loop1	46G	52M	44G	1%	/var/fireglass/upload
Tmpfs	1.6G	0	1.6G	0%	/var/cache/fireglass/content_cache

2. Decide what to delete from the full partition to be able to run the Symantec Threat Isolation system upgrade procedure successfully.

In the example above, the issue is with the partition `/var`. To identify the files that use the most disk space in this partition, run the following command:

```
sudo du --max-depth=1 -h /var
```



For example, if `/var/tmp` is very large, you can continue to run:

```
sudo du --max-depth=1 -h /var/tmp
```

Note that the `--max-depth` value can be extended incrementally to list subdirectories and their sizes to any required level of depth (for example, `--max-depth=2`). However, if, for example, `tmp` contains a very large subfolder called `x`, then it is better practice to run `--max-depth=1 -h /var/tmp/x`. Thus, the maximum depth will remain 1 and only the contents of `x` will be searched.

3. Identify the files that consume the most disk space and delete them.

9.3.4 Unauthenticated Users in Activity Logs

9.3.4.1 Cannot Find Activity Log Assigned to Specific User

An issue reported by a specific user does not seem to appear in the activity logs. This occurs when the user was not authenticated. A log for the issue exists, but the user was not authenticated because the rule did not require authentication.

The activity log displays the username only if a specific Access Role or “All authenticated users” was specified in the matched rule’s User field (see section [4.2.7 "Defining Policy Rules"](#)). If the User field is empty, the activity log will report “Unauthenticated”. For more information, see section [4.2.6 "Match Criteria Flow"](#).

It is recommended to try the following:

- If you know the source IP, try finding the log by source IP.
- If other logs exist for the same user, take their source IP and find logs with this source IP that do not include the user’s name.
- If you know the specific time that the issue occurred, try filtering by it.

9.3.4.2 All Activity Logs Have “Unauthenticated” Users

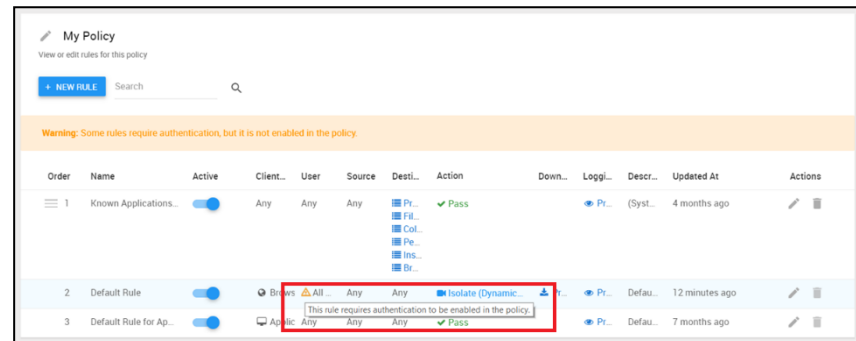
All activity logs show “Unauthenticated” users, rather than listing user names.

This occurs when the User field was left empty in the matched rule, meaning that the default option Any (including unauthenticated users) was selected. In this case, the rules can be matched without having to authenticate the user.



It is recommended to go to Policies → [Name of Your Policy] and verify the following:

- If the warning “Some rules require authentication, but it is not enabled in the policy” is displayed above the rules table, and the message “This rule requires authentication to be enabled in the policy” is displayed for the rule, under Actions click the edit icon for the policy and make sure that at least one Authentication setting is selected.



- If at least one Authentication setting is selected, make sure that either the option All authenticated users (the out-of-the-box Access Role), or the option One or more existing Access Roles is selected in some rules. Since the default option is Any (including unauthenticated users), it often occurs that this option is inadvertently selected in all rules.

9.3.4.3 Activity Log Displays “Generic User”

The activity log displays “Generic User” rather than the username.

This occurs when user authentication was skipped and authentication caching was configured to be done without identity. Symantec Threat Isolation allows the policy to be edited to include criteria for skipping authentication. When these criteria are matched, provided that the source egress IP address was authenticated previously, the user is considered trusted and authentication will be skipped.

The activity log displays “Generic User” instead of the user name when user authentication was skipped for unauthenticated requests. In this case, rules with a specific Access Role were skipped during matching. For more information, see section [4.2.2.2 "Authentication Mode"](#).