

ⓘ We're no longer updating this content regularly. Check the [Microsoft Product Lifecycle](#) for information about how this product, service, technology, or API is supported.

Recommended Version

✕



Firewall Rule Processing

Article • 08/26/2009

In this article


- Events
- Related Management Information

Applies To: Windows Server 2008 R2

Windows Firewall with Advanced Security receives its rules from local security policy stored in the system registry, and from Group Policy delivered by Active Directory. After receiving a new or modified policy, Windows Firewall must process each rule in the applied policies to interpret what network traffic is to be blocked, allowed, or protected by using Internet Protocol security (IPsec).

When appropriate auditing events are enabled (<https://go.microsoft.com/fwlink/?linkid=92666>), Windows reports successes and failures, both in retrieving policy and in processing the rules defined in the policy.

Events

 Expand table

Event ID	Source	Message
2002	Microsoft-Windows-Windows Firewall with Advanced Security	A Windows Firewall setting has changed. New Setting: %tType:%t%1 %tValue:%t%4 %tModifying User:%t%6 %tModifying Application:%t%7
2003	Microsoft-Windows-Windows Firewall with Advanced Security	A Windows Firewall setting in the %1 profile has changed. New Setting: %tType:%t%2 %tValue:%t%5 %tModifying User:%t%7 %tModifying Application:%t%8
2004	Microsoft-Windows-Windows Firewall with Advanced Security	A rule has been added to the Windows Firewall exception list. Added Rule: %tRule ID:%t%1 %tRuleName:%t%2 %tOrigin:%t%3 %tActive:%t%18 %tDirection:%t%6 %tProfiles:%t%11 %tAction:%t%10 %tApplication Path:%t%4 %tService Name:%t%5 %tProtocol:%t%7 %tSecurity Options:%t%21

		%tEdge Traversal:%t%19 %tModifying User:%t%22 %tModifying Application:%t%23"
2005	Microsoft-Windows-Windows Firewall with Advanced Security	A rule has been modified in the Windows Firewall exception list. Added Rule: %tRule ID:%t%1 %tRuleName:%t%2 %tOrigin:%t%3 %tActive:%t%18 %tDirection:%t%6 %tProfiles:%t%11 %tAction:%t%10 %tApplication Path:%t%4 %tService Name:%t%5 %tProtocol:%t%7 %tSecurity Options:%t%21 %tEdge Traversal:%t%19 %tModifying User:%t%22 %tModifying Application:%t%23"
2006	Microsoft-Windows-Windows Firewall with Advanced Security	A rule has been deleted in the Windows Firewall exception list. Deleted Rule: %tRule ID:%t%1% n%tRule Name:%t%2 %tModifying User:%t%3 %tModifying Application:%t%4
2008	Microsoft-Windows-Windows Firewall with Advanced Security	Windows Firewall Group Policy settings have changed. The new settings have been applied
2009	Microsoft-Windows-Windows Firewall with Advanced Security	The Windows Firewall service failed to load Group Policy. Error:%t%1
2010	Microsoft-Windows-Windows Firewall with Advanced Security	Network profile changed on an interface. Adapter GUID:%t%1 Adapter Name:%t%2 Old Profile:%t%3 New Profile:%t%4
2032	Microsoft-Windows-Windows Firewall with Advanced Security	Windows Firewall has been reset to its default configuration. %tModifyingUser:%t%1 %tModifyingApplication:%t%2
2033	Microsoft-Windows-Windows Firewall with Advanced Security	All rules have been deleted from the Windows Firewall configuration on this computer. %tStore Type:%t%1 %tModifyingUser:%t%2 %tModifyingApplication:%t%3
4946	Microsoft-Windows-Security-Auditing	A change has been made to Windows Firewall exception list. A rule was added. %t Profile Changed:%t%1 Added Rule: %tRule ID:%t%2 %tRule Name:%t%3
4947	Microsoft-Windows-Security-Auditing	A change has been made to Windows Firewall exception list. A rule was modified. %t Profile Changed:%t%1 Modified Rule:

		%tRule ID:%t%2 %tRule Name:%t%3
4948	Microsoft-Windows-Security-Auditing	A change has been made to Windows Firewall exception list. A rule was deleted. %t Profile Changed:%t%1 Deleted Rule: %tRule ID:%t%2 %tRule Name:%t%3
4949	Microsoft-Windows-Security-Auditing	Windows Firewall settings were restored to the default values.
4950	Microsoft-Windows-Security-Auditing	A Windows Firewall setting has changed. %t Profile That Was Changed:%t%1 New Setting: %tType:%t%2 %tValue:%t%3
4951	Microsoft-Windows-Security-Auditing	A rule has been ignored because its major version number was not recognized by Windows Firewall. %t Profile:%t%1 Ignored Rule: %tID:%t%2 %tName:%t%3
4952	Microsoft-Windows-Security-Auditing	Parts of a rule have been ignored because its minor version number was not recognized by Windows Firewall. The other parts of the rule will be enforced. %t Profile:%t%1 Partially Ignored Rule: %tID:%t%2 %tName:%t%3
4953	Microsoft-Windows-Security-Auditing	A rule has been ignored by Windows Firewall because it could not parse the rule. %t Profile:%t%1 Reason for Rejection:%t%2 Rule: %tID:%t%3 %tName:%t%4
4954	Microsoft-Windows-Security-Auditing	Windows Firewall Group Policy settings has changed. The new settings have been applied.
4956	Microsoft-Windows-Security-Auditing	Windows Firewall has changed the active profile. New Active Profile:%t%1
4957	Microsoft-Windows-Security-Auditing	Windows Firewall did not apply the following rule: Rule Information: %tID:%t%1 %tName:%t%2 Error Information: %tReason:%t%3 resolved to an empty set.
4958	Microsoft-Windows-Security-Auditing	Windows Firewall did not apply the following rule because the rule referred to items not configured on this computer:

		<p>Rule Information:</p> <p>%tID:%t%1</p> <p>%tName:%t%2</p> <p>Error Information:</p> <p>%tError:%t%3</p> <p>%tReason:%t%4</p>
5027	Microsoft-Windows-Security-Auditing	<p>The Windows Firewall Service was unable to retrieve the security policy from the local storage. The service will continue enforcing the current policy.</p> <p>Error Code:%t%1</p>
5028	Microsoft-Windows-Security-Auditing	<p>The Windows Firewall Service was unable to parse the new security policy. The service will continue with currently enforced policy.</p> <p>Error Code:%t%1</p>
5040	Microsoft-Windows-Security-Auditing	<p>A change has been made to IPsec settings. An Authentication Set was added.</p> <p>%t</p> <p>Profile Changed:%t%t%1</p> <p>Added Authentication Set:</p> <p>%tID:%t%t%t%2</p> <p>%tName:%t%t%t%3</p>
5041	Microsoft-Windows-Security-Auditing	<p>A change has been made to IPsec settings. An Authentication Set was modified.</p> <p>%t</p> <p>Profile Changed:%t%t%1</p> <p>Modified Authentication Set:</p> <p>%tID:%t%t%t%2</p> <p>%tName:%t%t%t%3</p>
5042	Microsoft-Windows-Security-Auditing	<p>A change has been made to IPsec settings. An Authentication Set was deleted.</p> <p>%t</p> <p>Profile Changed:%t%t%1</p> <p>Deleted Authentication Set:</p> <p>%tID:%t%t%t%2</p> <p>%tName:%t%t%t%3</p>
5043	Microsoft-Windows-Security-Auditing	<p>A change has been made to IPsec settings. A Connection Security Rule was added.</p> <p>%t</p> <p>Profile Changed:%t%t%1</p> <p>Added Connection Security Rule:</p> <p>%tID:%t%t%t%2</p> <p>%tName:%t%t%t%3</p>
5044	Microsoft-Windows-Security-Auditing	<p>A change has been made to IPsec settings. A Connection Security Rule was modified.</p> <p>%t</p> <p>Profile Changed:%t%1</p> <p>Modified Connection Security Rule:</p> <p>%tID:%t%t%t%2</p> <p>%tName:%t%t%t%3</p>
5045	Microsoft-Windows-Security-Auditing	<p>A change has been made to IPsec settings. A Connection Security Rule was deleted.</p> <p>%t</p> <p>Profile Changed:%t%1</p> <p>Deleted Connection Security Rule:</p> <p>%tID:%t%t%t%2</p> <p>%tName:%t%t%t%3</p>

5046	Microsoft-Windows-Security-Auditing	<div>A change has been made to IPsec settings. A Crypto Set was added. %t Profile Changed:%t%1</div> <div>Added Crypto Set: %tID:%t%t%t%2 %tName:%t%t%t%3</div>
5047	Microsoft-Windows-Security-Auditing	<div>A change has been made to IPsec settings. A Crypto Set was modified. %t Profile Changed:%t%1</div> <div>Modified Crypto Set: %tID:%t%t%t%2 %tName:%t%t%t%3</div>
5048	Microsoft-Windows-Security-Auditing	<div>A change has been made to IPsec settings. A Crypto Set was deleted. %t Profile Changed:%t%1</div> <div>Deleted Crypto Set: %tID:%t%t%t%2 %tName:%t%t%t%3</div>
5049	Microsoft-Windows-Security-Auditing	<div>An IPsec Security Association was deleted. %t Profile Changed:%t%1</div> <div>Deleted SA: %tID:%t%t%t%2 %tName:%t%t%t%3</div>

Related Management Information

[Windows Firewall Service](#)

[Windows Firewall with Advanced Security](#)