OKENA
71 Second Ave., 3rd Floor
Waltham, MA 02451

Phone 781 209 3200
Fax 781 209 3199

# StormWatch™

## Policies for StormWatch Managers Group

The policies shipped with StormWatch address both application-specific and environment-specific needs for servers and clients. In most cases, you'll want to use an application-specific policy in combination with an environment-specific policy to lock down a system with rules that are as restrictive or permissive as your network requires.

This document describes the StormWatch Manager policy shipped with the StormWatch Management Console. You can deploy this policy to protect your StormWatch server without making any changes to the policy itself. Use this document to understand what the policy currently does.

Use the following policies in combination to protect a StormWatch server.

| **Policy Name** | **Policy Description** |
|---|---|
| Common Security Module | V2.1 base policy module for all systems |
| Required Windows System Module | V2.1 policy module to allow critical Windows functions |
| Server Module | V2.1 base policy module for servers |
| StormWatch Manager Module | V2.1 policy module for StormWatch management servers |

## Policy Descriptions

The combined policies that are recommended for the protection of StormWatch server systems consist of rules which work in order of precedence. Access control rules, in particular, depend upon each other to lock down access to certain resources while providing specific open channels to allow access to other resources. The following section breaks out the combined access control rules by rule type in an attempt to help you understand how file access control rules (FACLs), for example, from each policy, work together once they are combined. Some FACLs allow access to certain files while others restrict access to other files. The same can be said about network access control rules and other access control rule types.

The following rule types are combined from the Common Security Module, Required Windows System Module, Server Module, and StormWatch Manager Module to protect StormWatch servers.

**File Access Control:**

- High Priority Deny - StormWatch server, read/write Cmd Shells
- High Priority Deny - StormWatch server, read/write SQL mgt Apps
- Allow - System bootstrap applications, read/write System executables, libraries and drivers
- Allow –(Disabled) Backup applications, read all files
- Allow - StormWatch manager helper apps, read/write to database
- Allow - StormWatch manager apps, read/write to config dir
- Allow - All Applications, read System libraries, drivers and data files
- Allow - Ensure access to DOS command line
- Query User - Installers, write System executables, libraries and drivers
- Query User - Virus scanners, write all files
- Query User - All applications, write privileged applications
- Query User - Installers, read/write user invoked executables and command shells
- Query User - All applications, write System executables, libraries and drivers
- Query User - Prevent access to system objects from downloaded scripts
- Query User- Protect writes to StormWatch manager configuration files
- Deny - vulnerable applications, read/write Cmd Shells

**Network Access Control:**

- Allow - Web browsers, client for HTTP services
- Allow - All applications, server for basic services
- Allow - All applications, client for basic services
- Allow - All applications, client for TCP and UDP service to Local Host
- Allow - All applications, server for TCP and UDP service from Local Host
- Allow - MS Security applications, client for TCP and UDP services
- Allow - MS Security applications, server for TCP and UDP services
- Allow - All applications, server for basic services
- Deny - All applications, server for TCP and UDP services

**Registry Access Control:**

- Allow - System applications, write keys typically targeted by viruses
- Query User - vulnerable applications, write keys typically targeted by viruses

Refer to the next section for descriptions of each individual rule and the purpose it serves in the policy in which it appears.

This section contains descriptions of the rules included in the sample policies recommended for deployment on a StormWatch server.

The rules that comprise these policies merge seamlessly and work in order of precedence. Policies should be combined (application-specific with environment-specific policies) to achieve the desired effect. They are broken out into separate categories so that they can be merged in various combinations and be used multiple times in multiple places.

| | |
|---|---|
| **Common Security Module** | V2.1 base policy module for all systems |

This policy enforces site-wide security practices. In general, security is either system-specific or application-specific. This policy is generic enough to be applied across your organization for protecting both systems and applications.

NOTE: This policy is applied to all StormWatch groups. However, it was not made “Mandatory” because it is up to administrators to determine whether this is a suitable corporate security policy or if it requires changes to meet more specific needs.

Also note that “vulnerable applications” defined in various rules are network-aware applications. These application types are much more vulnerable than others.

1. **File Access Control – Allow, System bootstrap applications, write System executables, libraries and drivers**

   Generally, writing to these resources should only occur when installing or uninstalling software. If StormWatch detects this action and you are not installing or uninstalling, this action is suspect. A wide variety of attacks try to compromise resources of this type. This rule is meant to allow targeted common actions denied by other restrictive rules in this policy.

2. **Registry Access Control – Allow, System applications, write keys typically targeted by viruses**

   This rule allows system applications to write to particular registry keys. Generally, writing to the registry keys specified in this rule should only occur when installing or uninstalling software. If StormWatch detects this action and you are not installing or uninstalling, this action is suspect. This rule is meant to allow targeted actions denied by other restrictive rules in this policy

3. **File Access Control – Query User (Default Allow), Installers, write System executables, libraries and drivers**

   This rule queries the user if known installation applications attempt to write to specified system resources. Generally, writing to these resources should only occur when installing or uninstalling software. If an installation is not taking place, this action should be denied.

4. **File Access Control – Query User (Default Allow), Virus scanners, write all files**

   This rule queries the user if known virus scanner applications are probing system files. Generally, writing to these resources should only occur when the system is being scanned for viruses. If this is not the case, this action should be denied.

5. **File Access Control – Query User (Default Allow), All applications, write privileged applications**

   This rule queries the user any if any applications are attempting to write to virus scanner applications or PDA applications. Generally, writing to these resources should only occur when these applications are being upgraded. If this is not the case, this action should be denied.

6. **File Access Control – Query User (Default Allow), Installers, user invoked executables and command shells**

   This rule queries the user if known installation applications attempt to write to specified user-invoked system resources. Generally, writing to these resources should only occur when installing or uninstalling software. If an installation is not taking place, this action should be denied.

7. **File Access Control – Query User (Default Deny), All applications, write System executables, libraries and drivers**

   This rule queries the user if any application attempts to write to system executables and specified libraries and drivers. Generally, writing to these resources should only occur when installing or uninstalling software. If StormWatch detects this action and you are not installing or uninstalling, this action is suspect. A wide variety of attacks try to compromise resources of this type. This rule is meant to maintain the integrity of the operating system.

8. **File Access Control – Query User (Default Deny), Prevent access to system objects from downloaded scripts**

   This rule queries the user if vulnerable applications attempt to write to the system disk.

9. **Registry Access Control – Query User (Default Deny), vulnerable applications, write keys typically targeted by viruses**

   This rule queries the user if any defined vulnerable applications attempt to write to particular registry keys. Generally, writing to the registry keys specified in this rule should only occur when installing or uninstalling software. If StormWatch detects this action and you are not installing or uninstalling, this action is suspect. This rule stops applications from being invoked or registering services, which is how viruses attempt to make themselves persistent.

10. **File Access Control – Deny, vulnerable applications, read/write Cmd Shells...**

    This rule prevents Web browsers and TCP and UDP-based applications from invoking commands shells which should generally only be invoked by users directly. (Web browsers and TCP and UDP-based applications are vulnerable to buffer-overflow attacks.)

11. **NT Event Log – All security related events**

    This rule provides added system security monitoring capabilities, causing all “security” NT event log messages to also appear in the StormWatch Management Console Event Log.

12. **Sniffer and protocol detection – Detect non-IP based protocols**

    This rule detects protocol stacks or drivers that interface with the network. You can modify this rule to detect any other network applications. This lets you monitor what is running on your network, such as packet sniffers that should not be running. If you have systems running sanctioned packet sniffer applications, you might want to exempt those applications from this rule or not apply this rule to that system to avoid false positive log messages.

| **Required Windows System Module** | V2.1 policy module to allow critical Windows functions |
|---|---|

This mandatory policy ensures that servers and desktops function properly and that StormWatch rules do not interfere with required system operations.

1. **File Access Control – Allow, All Applications, read System libraries, drivers and data files**

   This rule ensures that necessary applications can access system libraries and configuration files needed for startup purposes and other general operations.

2. **File Access Control – Ensure access to DOS command line**

   This rule ensures that the DOS prompt does not become a restricted application as a result of receiving a downloaded content designation.

3. **Network Access Control – Allow, MS Security applications, server for TCP and UDP services**

   This rule lets Microsoft's security subsystem communicate on the network, allowing for authentication and authorization services, e.g. Kerberos and LDAP.

4. **Network Access Control – Allow, All applications, server for TCP and UDP service from Local Host**

   This rule allows various applications running on the same system to talk to each other while still denying access to these services from other non-localhost applications. This improves system performance by allowing all local applications to attempt to access all needed local resources as a server.

5. **Network Access Control – Allow, MS Security applications, client for TCP and UDP services**

   This rule lets Microsoft's security subsystem communicate on the network, allowing for authentication and authorization services, e.g. Kerberos and LDAP.

6. **Network Access Control – Allow, All applications, client for basic services**

   This rule ensures that applications can perform functions such as name resolution and endpoint mapping.

7. **Network Access Control – Allow, All applications, server for basic services**

   This rule ensures that applications can act as a server for functions such as WINS and endpoint mapping.

8. **Network Access Control – Allow, All applications, client for TCP and UDP service to Local Host**

   This rule allows various applications running on the same system to talk to each other while still denying access to these services from other non-localhost applications. This improves system performance by allowing all local applications to attempt to access all needed local resources as a client.

| **Server Module** | V2.1 base policy module for servers |
|---|---|

This policy provides system hardening features for servers.

1. **File Access Control - (Disabled) Allow, Backup applications read all files**

   This rule is included in the Base Server policy, but it is disabled by default. Enable and use this policy to allow file backups. If you are backing up files over the network, you will have to add a Network Access Control rule as well.

2. **Syn flood protection**

   SYN flooding is a type of denial of service attack. It occurs in TCP/IP communications when connection requests are received from forged addresses (non-existing machines). This results in half open connections on the server. An abundance of half open states on a server can prevent legitimate connections from being established. Using SYN flood protection in a policy prevents this attack from succeeding. You should apply SYN flood protection to servers within your enterprise, keeping them up and running and able to provide resources should a SYN flood attack occur.

3. **Portscan detection - Detect network portscans**

   Portscanning is a common method for finding weaknesses at a site by determining what network services are being run. An attacker attempts to connect to port after port on a target system until a vulnerable service is found. Using portscan detection in a policy causes the intelligent agent on a protected system to log an event (one per minute) when an attempt is made to scan the system for an open port. This can warn you if someone is mapping out your system in preparation for an attack. The intelligent agent also gathers information on the number of different source IP addresses perpetrating the scan and it reveals the source address of the latest scan attempt. If scans are detected across several machines, StormWatch correlates these events and generates an additional event to warn of this correlation.

4. **Trojan detection - Detect and terminate potential application Trojans**

   Trojans are a form of malicious programming code that runs undetected on a machine and can allow an attacker to steal information or control the system in some manner. Use StormWatch's Trojan detection rule in a policy to detect and prevent Trojans from performing malicious acts on individual systems and networks.

| StormWatch Manager Module | V2.1 policy module for StormWatch management servers |
|---|---|

This policy protects the StormWatch server application, both granting permissions and imposing restrictions.

1. **File Access Control – High Priority Deny, StormWatch server, read/write Command Shells**

   This rule takes precedence over all other rules in this policy. It stops the StormWatch server application from reading or writing any command line shell executables such as cmd.exe and bash.exe. Additionally, StormWatch makes use of third party software such as MS SQL Server Database and Crystal Reports. This rule protects these third party services from buffer-overrun attacks.

2. **File Access Control – High Priority Deny, StormWatch server, read/write SQL mgt Apps**

   This rule prevents third party applications used by StormWatch from accessing local administration applications for SQL server. This would prevent the management system from being compromised in the event of a buffer overflow attack.

3. **File Access Control – Allow, StormWatch manager helper apps, allow writes to database**

   This rule allows third party applications used by the StormWatch server write to the StormWatch database. This access is locked down by other deny rules in this policy.

4. **File Access Control – Allow, StormWatch manager apps, allow writes to config dir**

   This rule allows third party applications used by the StormWatch server write to the StormWatch configuration directory. This access is locked down by other deny rules in this policy.

5. **Network Access Control – Allow, Web browsers, client for HTTP services**

   This rule allows the administrator to access the StormWatch Management Console locally on the server itself. This access not locked down by any other existing rules. It is provided as accessibility insurance for the StormWatch server if any network policies are applied to it that inadvertently block this local HTTP access.

6. **Network Access Control – Allow, All applications, server for basic services**

   This rule allows all applications to act as a server for basic network services such as NetBIOS Name Service. These services are denied by rule 6. This rule opens a targeted channel in that rule, allowing the system to communicate over the network using only specified services.

7. **File Access Control – Query User, Protect writes to Stormwatch manager configuration files**

   This rule queries the user if any application attempts to write to specified StormWatch system resources. Generally, writing to these resources should only occur when installing or updating StormWatch software. If an installation is not taking place, this action should be denied.

**8. Network Access Control – Deny, All applications, server for TCP and UDP services**

This rule locks down the system, preventing it from acting as a server for specified services. This prevents unauthorized servers from accepting incoming connections and prevent applications that are potentially malicious, and are running without your knowledge, from compromising your machine. This stops unauthorized applications from talking on the network.