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

Phone 781 209 3200
Fax 781 209 3199

StormWatch™

Policies for Default Desktops 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 combination of policies shipped with the StormWatch Management Console to protect user desktop systems. You can deploy these policies to protect desktop systems without making any changes to the policies themselves. It is recommended that you do not edit these policies, but instead add new policies for any changes you might require. Use this document to understand what the policies currently do and then decide if it suits your network's needs. Use the following policies in combination to protect the majority of client desktops across your enterprise.

Policy Name	**Policy Description**
Common Security Module	V2.1 base policy module for all systems
Desktop Module	V2.1 base policy module for desktops
Inbound Port Blocking Module	V2.1 policy module to block incoming connections
Distributed Firewall Module (optional)	V2.1 policy module to restrict network services
Instant Messenger Module	V2.1 policy module for Instant Messenger
Microsoft Office Module	V2.1 policy module for Microsoft Office
Required Windows System Module	V2.1 policy module to allow critical Windows functions

Policy Descriptions

The combined policy modules that are recommended for the protection of desktop 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, Desktop Module, Inbound Port Blocking Module, Instant Messenger Module, Microsoft Office Module, and Required Windows System Module to protect desktops.

File Access Control:

- High Priority Deny - Email applications, read/write dynamically quarantined files
- High Priority Deny - Email applications, read/write user invoked applications and command shells
- Allow - System bootstrap applications, read/write System executables, libraries and drivers
- Allow - Microsoft Office and descendents, read/write non-executable files
- Allow - WinZip applications, read/write Microsoft Office files
- Allow - Instant Messenger applications, read Instant Messenger directories
- Allow –(Disabled) Backup applications, read all files
- 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 Instant Messenger executables
- Query User - All applications, write System executables, libraries and drivers
- Query User - Prevent access to system objects from downloaded scripts
- Query User - All applications, write MS Office executables
- Query User – Processes reading downloaded content, write MS Office data files
- Query User - Instant Messenger applications, read/write Suspicious Email files
- Query User - Email applications, read/write Suspicious Email files
- Deny - Email applications, read/write Cmd Shells
- Deny - vulnerable applications, read/write Cmd Shells
- Deny - Microsoft Office and descendents, write all executables
- Deny - Instant Messenger applications, write any executable file type

Network Access Control:

- Allow - All applications, client for TCP with Data Connections and UDP services
- Allow - All applications, server for SMB services (offering network shares)
- Allow - Microsoft Office, client for HTTP service
- Allow - Instant Messenger applications, client Instant Messenger service (AOL and MSN)
- Allow – Instant Messenger applications, client HTTP service (Yahoo)
- Allow – (Disabled) Instant Messenger applications, client Email, NNTP, MMCC services (Yahoo)
- Allow - All applications, client for basic services
- Allow - All applications, server 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
- 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
- Query User - All applications, write MS Office security keys

COM Component Access Control:

- Allow - Microsoft Office applications, access to MS Office objects
- Allow - Email and web applications, access to MS Office objects
- Allow - PDA applications, access outlook
- Deny - Vulnerable applications and Windows Scripting Host, accessing outlook

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

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.

This section contains descriptions of the rules included in the sample policies recommended for deployment on most client desktops.

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.

Desktop Module	V2.1 base policy module for desktops

This policy protects the operating system and most client applications, both granting permissions and imposing restrictions.

1. **File Access Control – High Priority Deny, Email applications, read/write dynamically quarantined files**

   This rule denies all specified email applications from attempting to read or write any files that appear on the StormWatch dynamic quarantined file list. This is the rule that prevents email clients from opening dynamically quarantined files and it must be used in conjunction with the Network Worm Protection rule which is included in this policy.

   The quarantined file list is a temporary one. To permanently block specific, dangerous files, you can create a file set of these files and use them in a deny rule.

2. **File Access Control – High Priority Deny, Email applications, read/write user invoked applications and command shells**

   This rule prevents email applications from reading or writing any command line shell executables such as cmd.exe and bash.exe. This prevents buffer-overrun attacks from invoking arbitrary commands on a system via a shell. Email applications are common client networking software. If clients are running other networking software, you could add that software to the application class for inclusion in this rule.

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

   This rule is included in the Desktop Module, 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.

4. **COM Component Access Control – Allow, PDA applications, access outlook**

   This rule allows PDA applications to access the outlook mail address books. This access is denied by another COM rule in this policy. This rule opens a targeted hole in that deny rule.

5. **File Access Control – Query User (Default Deny), Email applications, read/write Suspicious Email files.**

   This rule queries the user if any specified email applications attempt to read or write suspicious email files. Suspicious email files are any files matching commonly known virus naming patterns.

6. **COM Component Access Control – Deny, Vulnerable applications and Windows Scripting Host, accessing outlook**

   This rule denies vulnerable applications and the Windows Scripting host from accessing any Microsoft Outlook Com components. For example, this prevents a VBS-based virus from accessing your address book and making outgoing connections.

7. Network Worm Protection – Detect and protect against network worms

Email worms are one of the most commonly spread and costly viruses affecting corporate networks today. The most recent worms of note were the ILOVEYOU and Melissa mail worms and variations thereof. When this type of suspicious activity is detected, the intelligent agent queries the user, informing the user of this activity. When the user selects to stop the system action in question on the desktop where the worm is received, the network worm is prevented from propagating itself. The preconfigured StormWatch network worm protection rule also correlates a series of suspicious events across multiple machines. Network correlation detection of a worm quarantines the file in question, ensuring that no other users receive it.

8. NT Event Log – Integrate Norton AV events

This rule provides extra desktop system monitoring capabilities, causing any “Norton AntiVirus” NT event log messages to also appear in the StormWatch Management Console Event Log.

9. 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.

10. 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.

Inbound Port Blocking Module	V2.1 policy module to block incoming connections

This policy controls network accessibility, allowing most client applications to run and preventing server software from running on client desktops. This blocks Trojans and viruses that act as servers and try to invoke malicious code on compromised machines.

(To lock down client services further, you can use the Distributed Firewall Module, explained later in this document, or the Network Lockdown Module. If you do further restrict network services, some client applications will no longer run.)

1. **Network Access Control – Allow, All applications, client for TCP with Data Connections and UDP services**

   This rule allows most client services with callback connections (such as FTP) to run.

2. **Network Access Control – Allow, All applications, server for SMB services (offering network shares)**

   This rule allows all applications to offer network shares to local system directories.

3. **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 systems from accepting incoming connections and stops applications that are potentially malicious, and are running without your knowledge, from compromising your machine. Rules 1 and 2 open targeted channels in this rule.

Optionally, you can use the Distributed Firewall Module as part of your Default Desktop group set rather than the Inbound Port Blocking Module. This allows you to enumerate which services are allowed to run on client desktops, restricting network access to a greater degree. The Distributed Firewall Module shipped with StormWatch provides an example of explicitly enumerated services.

The advantage of enumerating which services are allowed to run on a system is that you can specify authorized protocols and then tie them to authorized applications. This prevents arbitrary programs from using legitimate applications to perform malicious acts. For example, this policy contains a rule allowing only specific email applications to receive email traffic over authorized protocols. An unauthorized mail client cannot access email.

Distributed Firewall Module	V2.1 policy module to restrict network services

This policy controls network accessibility, allowing most client applications to run and preventing server software from running on client desktops. This blocks Trojans and viruses that act as servers and try to invoke malicious code on compromised machines.

1. **Network Access Control – Allow, Web browsers, client for HTTP, FTP and Real Audio services**

   This rule allows Web browsers access to most commonly used services.

2. **Network Access Control – Allow, All applications, client for SMB services (connecting to network shares)**

   This rule allows all applications to connect to network shares. These services are denied by other rules in this policy. This rule opens a targeted channel for network shares.

3. **Network Access Control – Allow, All applications, client for Time Protocol Service**

   This rule allows all applications to use time protocols over the network to maintain accurate synchronized time across machines.

4. **Network Access Control – Allow, All applications, server for SMB services (offering network shares)**

   This rule allows all applications to offer network shares to local system directories. These services are denied by other rules in this policy. This rule opens a targeted channel for network shares.

5. **Network Access Control – Allow, Email applications, client for Mail and LDAP services**

   This rule allows defined email applications to access the network to receive email and to access directory services.

6. **Network Access Control – Allow, Print Spool applications, client for TCP and UDP services)**

   This rule allows defined print spools applications to access a network printer.

7. **Network Access Control – Allow, Multimedia applications, client for HTTP and Real Audio services**

   This rule allows defined multimedia applications to act as a client for defined HTTP and Real Audio protocols.

8. **File Access Control – Query User (Default Deny), All applications, write Email and Web Browser client executables**

   This rule queries the user if any applications attempt to write to email and web browser application executable files. This rule prevents malicious code from impersonating authorized network programs.

9. **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 systems from accepting incoming connections and stops applications that are potentially malicious, and are running without your knowledge, from compromising your machine. Rules # and # open targeted channels in this rule.

10. **Network Access Control – Deny, All applications, client for TCP and UDP services**

    This rule locks down the system, preventing it from acting as a client for specified services. This prevents unauthorized systems from making outgoing connections.

Instant Messenger Module	V2.1 policy module for Instant Messenger

This policy allows Instant Messenger applications to run on desktops while it secures those applications, controlling what operations they can perform on systems.

1. **Network Access Control – (Disabled) Allow, Instant Messenger applications, client Email, NNTP, MMCC services (Yahoo)**

   By default, this rule is disabled. You can enable it to allow specified instant messenger applications to act as a client for receiving email, communicating with newsgroups, and using additional Yahoo messenger services. This rule is disabled because some administrators may not consider instant messenger applications to be an appropriate client for the services listed in this rule.

2. **File Access Control – Allow, Instant Messenger applications, read Instant Messenger directories**

   This rule allows the instant messenger application to read and write to its own data files. This access is locked down by deny rules in this policy.

3. **Network Access Control – Allow, Instant Messenger applications, client HTTP service (Yahoo)**

   This rule allows Yahoo's instant messenger application to act as a client for HTTP services. Yahoo requires this access to operate.

4. **Network Access Control – Allow, Instant Messenger applications, client Instant Messenger service (AOL and MSN)**

   This rule allows instant messenger applications to make use of AOL and MSN proprietary instant messaging protocols. AOL and MSN require this access to operate.

5. **File Access Control – Query User (Default Deny), All applications, write Instant Messenger executables**

   This rule protects the instant messenger service executables, querying users to prevent applications from overwriting the executables themselves. This would prevent a Trojan from posing as the instant messenger service. (This rule will also trigger when you are upgrading instant messenger software. In that case, you would answer Yes to the query to allow the upgrade.)

6. **File Access Control – Query User (Default Deny), Instant Messenger applications, read/write Suspicious Email files**

   Instant messenger applications can be used as email clients and to transfer files. Therefore, this rule causes the user to be queried if an instant messenger application attempts to read or write to a known suspicious email file.

7. **File Access Control –Deny, Instant Messenger applications, write any executable file type**

   This rule stops the instant messenger application from downloading executable files types.

Microsoft Office Module	V2.1 policy module for Microsoft Office

This policy protects Microsoft Office applications.

1. **COM Component Access Control – Allow, Microsoft Office applications, access to MS Office objects**

   This rule allows specified Microsoft Office applications to access office-related COM components.

2. **COM Component Access Control – Allow, Email and web applications, access to MS Office objects**

   This rule allows specified email and web applications to access office-related COM components.

3. **File Access Control – Allow, WinZip applications, read/write Microsoft Office files**

   This rule allows MS Office documents to be compressed into and extracted from WinZip files. (If you are using software other than WinZip to perform these functions, you must include that software in this rule.)

4. **File Access Control – Allow, Microsoft Office and descendents, read/write non-executable files**

   This rule allows the MS Office application and its descendents read and write to files that are not executables, libraries or drivers. This allows MS Office to access the files it requires to operate while protecting the system files that are restricted by other rules.

5. **Network Access Control – Allow, Microsoft Office, client for HTTP services**

   This rule allows MS Office applications to connect as a client to HTTP services. Because several MS Office applications provide the ability to include links to web sites in documents and to save documents as HTML files, this access is needed to utilize these features.

6. **File Access Control – Query User (Default Deny), All applications, write Microsoft Office executables**

   This rule protects the Microsoft Office application executables, querying users if applications are attempting to overwrite the executables themselves. This would prevent a Trojan from posing as a Microsoft Office application. This should only occur legitimately if users are upgrading software.

7. **File Access Control – Query User (Default Deny), Processes reading downloaded content, write MS Office data files**

   This rule queries the user if any processes that are seen as having read downloaded content write to particular Microsoft Office files. For example, this would prevent a downloaded virus from deleting documents on your disk. If you want to prevent someone from stealing documents off a system disk, you can change this rule to prevent read access as well.

8. **Registry Access Control – Query User (Default Deny), All applications, write MS Office security keys**

   This rule protects the application's security-related registry keys, querying users when applications attempt to write to them and attempt to change the MS Office security configuration. For example, this would stop a virus from disabling MS Office macro protection.

9. **File Access Control – Deny, Microsoft Office and descendents, write all executables**

   This rule stops the Microsoft Office application and any processes it spawns from writing to executable files types. For example, this rule would prevent a macro virus infection on a system.

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. (This rule does not allow for network shares. Other rules, such as those found in the Default Desktop policy, provide that added service.)

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.