



# **Fireware XTM**

## **Getting Started with Application Control v11.4.1**

---

## About this Getting Started Guide

---

The *Getting Started with Application Control* guide is updated with each major product release. For the most recent product documentation, see the *Fireware XTM WatchGuard System Manager Help* or *Fireware XTM Web UI Help* on the WatchGuard web site at:

<http://www.watchguard.com/help/documentation/>.

Information in this guide is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without the express written permission of WatchGuard Technologies, Inc.

Guide revised: 4/5/2011

## Copyright, Trademark, and Patent Information

---

Copyright © 1998-2011 WatchGuard Technologies, Inc. All rights reserved. All trademarks or trade names mentioned herein, if any, are the property of their respective owners.

Complete copyright, trademark, patent, and licensing information can be found in the Copyright and Licensing Guide, available online at: <http://www.watchguard.com/help/documentation/>.



This product is for indoor use only.

---

### About WatchGuard

WatchGuard offers affordable, all-in-one network and content security solutions that provide defense-in-depth and help meet regulatory compliance requirements. The WatchGuard XTM line combines firewall, VPN, GAV, IPS, spam blocking and URL filtering to protect your network from spam, viruses, malware, and intrusions. The new XCS line offers email and web content security combined with data loss prevention. WatchGuard extensible solutions scale to offer right-sized security ranging from small businesses to enterprises with 10,000+ employees. WatchGuard builds simple, reliable, and robust security appliances featuring fast implementation and comprehensive management and reporting tools. Enterprises throughout the world rely on our signature red boxes to maximize security without sacrificing efficiency and productivity.

For more information, please call 206.613.6600 or visit [www.watchguard.com](http://www.watchguard.com).

### Address

505 Fifth Avenue South  
Suite 500  
Seattle, WA 98104

### Support

[www.watchguard.com/support](http://www.watchguard.com/support)  
U.S. and Canada +877.232.3531  
All Other Countries +1.206.521.3575

### Sales

U.S. and Canada +1.800.734.9905  
All Other Countries +1.206.613.0895

# Table of Contents

---

<b>Introduction</b> .....	<b>1</b>
Does your company have a policy for the appropriate use of applications?.....	1
<b>How Application Control Identifies Applications</b> .....	<b>2</b>
<b>Application Control — Begin with Monitoring</b> .....	<b>3</b>
Monitor Application Use.....	3
Run Application Control Reports.....	4
<b>Block an Application</b> .....	<b>5</b>
<b>Policy Guidelines for Application Control</b> .....	<b>7</b>
Global Application Control Action.....	8
Performance Implications.....	8
<b>Use Application Categories</b> .....	<b>9</b>
Override a Category Action.....	11
<b>Application Control and Proxies</b> .....	<b>11</b>
<b>Application Control and WebBlocker</b> .....	<b>12</b>
<b>Manage SSL Applications</b> .....	<b>12</b>
<b>Manage Applications that Use Multiple Protocols</b> .....	<b>13</b>
<b>Monitor Downloads and File Transfers</b> .....	<b>13</b>
<b>Manage Facebook Applications</b> .....	<b>13</b>
<b>Application Control Policy Examples</b> .....	<b>15</b>
Allow an Application For a Group of Users.....	15
Block Applications During Business Hours.....	16
<b>For More Information</b> .....	<b>17</b>



# Introduction

---

Unlimited use of applications in business today presents a number of security, compliance, and productivity issues.

- Social networking and Web 2.0 applications present new ways for malware and threats to enter an organization.
- Important information can leak from organizations through unauthorized channels (e.g. file transfer over instant messaging).
- Employees can waste company time on social networking and online games.
- Employees can use bypass proxies to avoid firewall controls.
- Many applications represent dangerous threat vectors, often associated with malware which can enter and damage corporate networks.

But many web applications, such as Facebook, are now required for legitimate business reasons. For example, over 1.5 million small businesses use Facebook to get their message out to their customers.

WatchGuard has introduced a comprehensive new service in Fireware XTM v11.4 that allows you to define which applications can be used in your organization, by whom, and when. With Application Control, you can exercise fine-grained control over more than 1,500 applications, organized by category. Companies can establish acceptable use policies for users and groups by category, application, and application behaviors for maximum flexibility. The product provides comprehensive reports that can be used to demonstrate compliance, evaluate employee need, and enforce acceptable use policies.

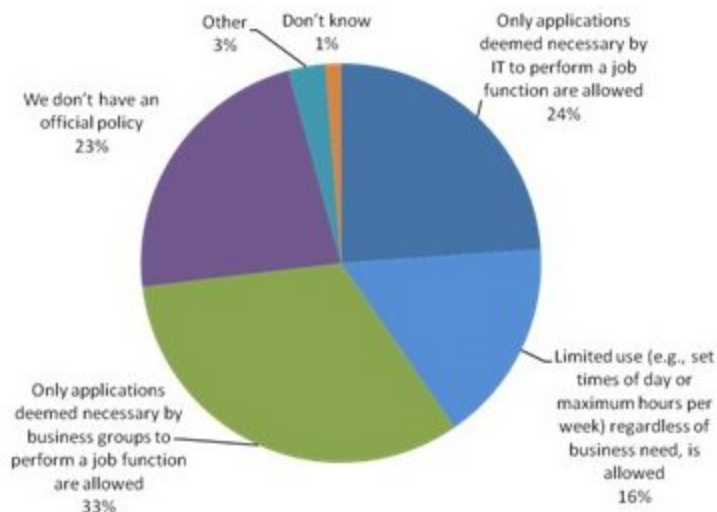
But as an administrator, where do you start?

This document describes practical details to consider in your implementation of WatchGuard's powerful new subscription service.

## **Does your company have a policy for the appropriate use of applications?**

As with any new security control, the best place to start is with your own security policy. Application Control provides an excellent tool to help you define, enforce, and audit a corporate acceptable use policy. But before you rush to configure settings in the product, you need to consider whether the company already has a policy that needs to be enforced. Have the employees been educated, and are they aware of what is considered appropriate use? The chart below from Forrester Research shows that 23% of companies do not have any official policy in place to govern the usage of Web 2.0 applications.

**“Which of the following best describes your firm’s official IT policy for acceptable use of consumer-oriented collaboration tools and Web 2.0 applications?”**



**Base: 1,033 SMB & enterprise IT security decision makers**  
**Source: Forrester Research, Forrsights Security Survey, Q3 2010**

If your company does not have a policy in place that governs application use, you certainly do not want to start by blocking applications immediately. It is probably more appropriate to start with logging and reporting of application use. Work with stakeholders in your organization to develop a policy that clearly states your company’s goals.

If your company already has a policy in place, you might want to look at options to make the policy more granular and specific. Again, logging and reporting might be the best first step. Make sure you have a good understanding of the applications that are used in the organization before you set up any rules that block traffic.

For example, consider these questions:

- Is there a broad policy in place that needs to get more specific now?
- Does the business need to limit application use by time of day, or specific business group?

## How Application Control Identifies Applications

---

Application Control uses several methods to identify traffic associated with specific applications:

- Simple pattern matching of patterns in the packets.
- Simple L4 port-based rules for applications in the Network Protocols category. Applications can be identified by their use of well known ports.
- Examination of the SSL certificates that are used.
- Behavior correlation of related signatures. When the first few packets arrive, Application Control can identify that the traffic is Facebook. As it examines more packets, it could further identify the traffic as a Facebook application.

The most complex applications to identify are applications such as Skype that use their own implementation of encrypted communication. Unlike other VoIP applications, Skype is based on peer-to-peer technology. There is no central infrastructure. The entire Skype directory of users is distributed among all the nodes in the network. Once a user registers with the service and downloads the client, their system could potentially become a node in the network, even if it is not actively making a call. Skype was designed to get around firewalls and it dynamically uses a combination of ports.

Together with signatures, Application Control uses a patent pending algorithm to identify these encrypted applications such as Skype, Winny, and Thunder. Application Control examines traffic characteristics such as packet sizes, patterns of DNS lookups, and the patterns of different ports that are used.

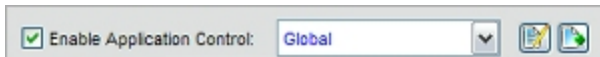
## Application Control — Begin with Monitoring

When you start to use Application Control, we recommend that you first configure your policies to send log messages for all application use so that you get a true understanding of the applications that are used on the network. To monitor application use, you can enable Application Control and logging for all policies that match the application traffic. After you enable Application Control and logging for a policy, all application activity for traffic through that policy is recorded in the log database and available for the Application Control reports, even if the Global Application Control action is empty.

### Monitor Application Use

To monitor application use:

1. Create an Application Control action that does not block any applications.  
*The Global action is empty by default, so it does not block applications.*
2. Apply the empty Application Control action to the policies that handle traffic you want to monitor.



For information about which policies to configure, see [Policy Guidelines for Application Control](#).

3. Enable logging in each policy that has Application Control enabled.

For information about how to enable logging in a policy, see the Fireware XTM WatchGuard System Manager or Fireware XTM Web UI User Guides or Help systems.



If you do not enable logging for a policy that has Application Control enabled, Application Control saves log information only for blocked applications.

## Run Application Control Reports

After you have enabled Application Control and logging in your policies, you can use Report Manager to run Application Control reports that summarize information about the applications used on your network.

Report Manager includes these predefined reports for Application Control:

### Application Control Reports

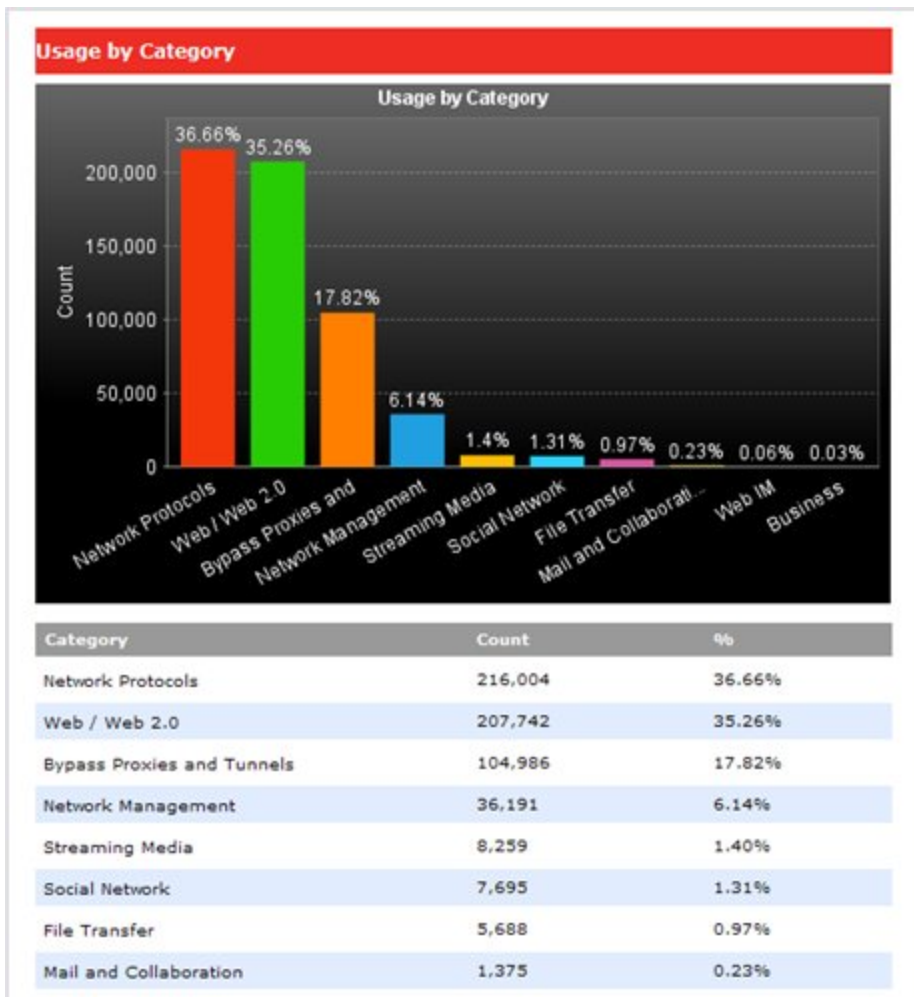
- Application Usage Summary
- Blocked Application Summary

### Client Reports — Show which users use the applications

- Top Clients by Application Usage
- Top Clients by Blocked Applications
- Top Clients by Blocked Categories

Client reports show the names of users who use applications if you have configured authentication on the firewall.

Before you configure Application Control to block applications, we recommend that you examine the Application Usage Summary and the Top Clients by Application Usage reports.



When you look at the Application Usage reports, consider these questions:

- Does the report show any application categories that seem to conflict with corporate policy?
- Are the applications appropriate for business use?
- Which users use the applications? Fireware XTM provides reports that show application use by client. The authentication capabilities in Fireware XTM enable you to see client reports by user name rather than by IP address. You can also identify user traffic in Terminal Services environments.

For more information about how to configure Terminal Services, see the Fireware XTM v11.4 User Guide or Help.

If the reports show an application that you are not familiar with, you can look up information about the application on the WatchGuard Application Control Security Portal at <http://www.watchguard.com/SecurityPortal/AppDB.aspx>.



WatchGuard also provides a Security Portal with information about the Intrusion Prevention Service signatures at: <http://www.watchguard.com/SecurityPortal/ThreatDB.aspx>.

## Block an Application

With Application Control, you can quickly and easily block access to many applications.

To block an application, you simply edit the Application Control action, select the application you want to block, and set the action for that application to **Drop**. After you have configured your Application Control action to block applications, you can then apply that Application Control rule to policies in your configuration.

For example, to configure Application Control to block the MSN instant messaging application:

1. Edit an Application Control Action. You can edit the predefined **Global** Application Control action or create a new one.
2. In the **Search** text box, type the name of the application you want to block. In this example, type **MSN**.

**New Application Control Action**

Name:

Description:

Show all applications

Show only configured applications Category:  Search:

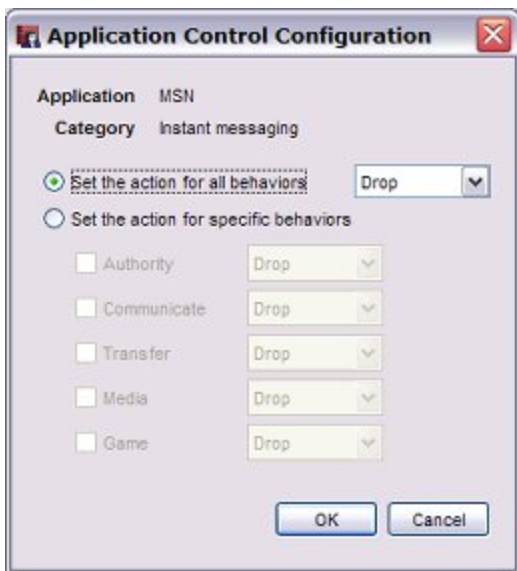
Category	Application	Behavior	Action
Instant messaging	MSN	Authority, Communicate...	
Web / Web 2.0	MSN Money	Authority, Access	
Web IM	MSN2GO Web IM	Authority, Access	
Web IM	MSN Web Messenger	Authority, Communicate	

Select by Category... Clear Action Edit...

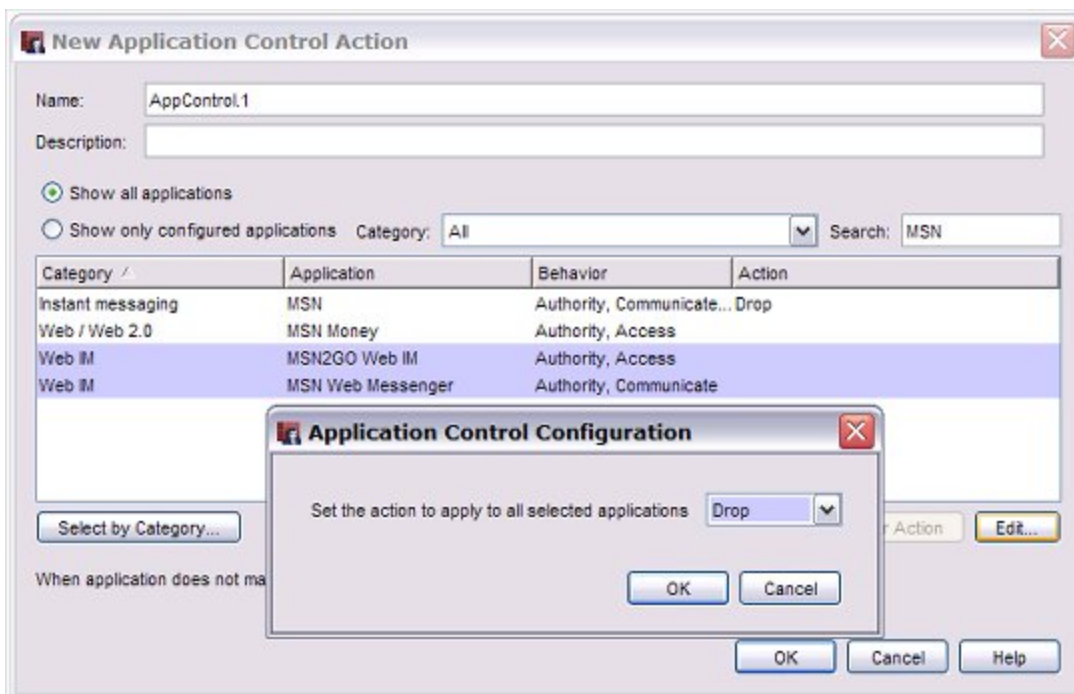
When application does not match:

OK Cancel Help

- 3. In the application list, select the MSN application. Click **Edit**.



- 4. Set the action for all behaviors to **Drop**.
- 5. Click **OK**.
- 6. If you also want to block MSN Web Messenger and MSN2GO Web IM applications, select those two applications, then click **Edit**.



Now you can apply this Application Control action to policies in your configuration. Policy configuration is discussed in the next section.

## Policy Guidelines for Application Control

---

To monitor or block application use, you must enable Application Control for all policies that handle the application traffic. We do not recommend that you apply the Global Application Control action to every policy. Because of the performance implications, you don't want — or need — to enable Application Control for every policy.

We recommend that you enable Application Control for these types of policies:

- Any outbound policy that handles HTTP or HTTPS traffic
- VPN policies that use 0.0.0.0/0 routes (default-route VPNs)
- Any outbound policy if you are not sure how the policy is used
- Policies that use the 'Any' protocol
- Policies that use an 'Any-\*' alias, for example Allow 'Any-Trusted' to 'Any-External', on a specific port/protocol

It is not necessary to enable Application Control for a policy if you control the network on both sides of a traffic flow the policy handles. Some examples of these types of policies include:

- POS systems
- Intranet web applications
- Internal databases and traffic in a DMZ

It is not usually necessary to enable Application Control for policies that are restricted by port and protocol and that allow only a known service. Some examples of these types of policies include:

- Default WatchGuard policies
- DNS traffic
- RDP
- VoIP - SIP and H.323 application layer gateways

Each policy can allow only the traffic that matches the protocol for that policy. For example, HTTP application traffic is never allowed through the DNS proxy. To effectively monitor or block an application, you must consider all protocols used by that application, and enable Application Control for all policies that handle those protocols.

To block evasive applications that dynamically use different ports, you must enable Application Control to block those applications in all of your policies. For more information about evasive applications, see the [Fireware XTM User Guide](#) or [Help](#).

For some examples of how to use Application Control with policies, see [Application Control Policy Examples](#).

## Global Application Control Action

The Global Application Control action is created by default and cannot be removed. You can configure the Global Application Control action to control overall corporate policy. For example you can:

- Block all games
- Block use of peer-to-peer applications

The Global Application Control action does not apply to traffic unless you enable Application Control for policies in your configuration. You can assign the Global Application Control action directly to a policy, or you can use the Global Application Control action as a secondary action if traffic does not match the applications configured in a user-defined Application Control action assigned to a policy.

You can create more specific application actions to implement rules that apply to user groups or to specific interfaces. For example, you might want to apply some specific rules to allow one department to have access to an application.

If you know that an application is specifically restricted to a specific port, you can apply an Application Control action to a packet filter or proxy policy on that port only. If not, you must apply the Application Control action to an outgoing policy that covers all ports to make sure that you capture all possible traffic for the application.

## Performance Implications

Application Control does not impact firewall throughput when it is not enabled for any policies.

If IPS is already enabled, the performance impact when you enable Application Control is not significant, because IPS already performs deep inspection of the packets that pass through the firewall.

After you configure the Application Control action and apply it to policies, you can expect to see a performance impact if IPS is not already configured. Throughput could drop to 20% - 40% of the firewall throughput without any deep inspection. Throughput rates vary based on your environment and configuration.

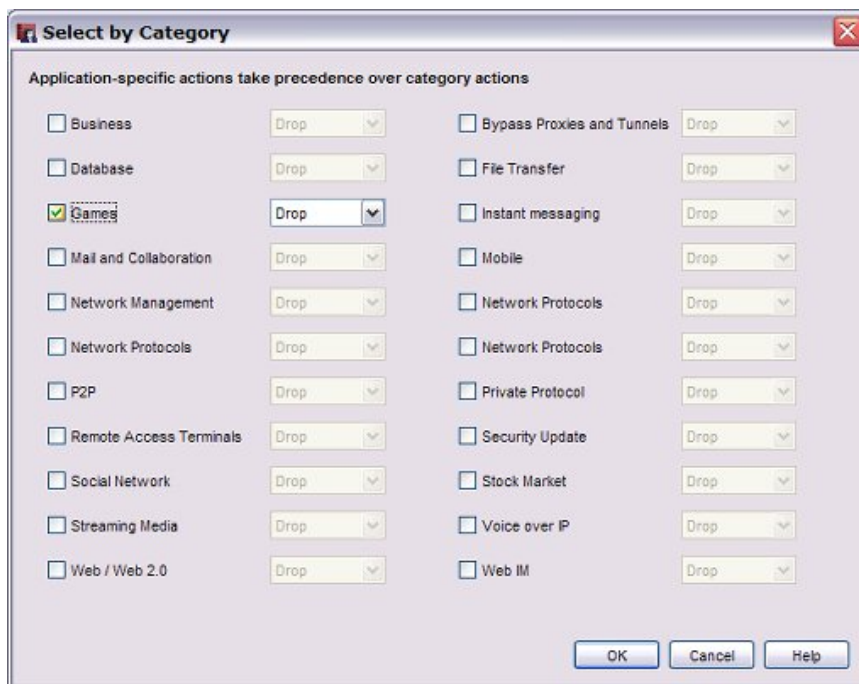
Performance is not affected by the number of applications configured in an Application Control action. There is not a significant performance difference whether you configure 50 or 500 applications in an Application Control action.

## Use Application Categories

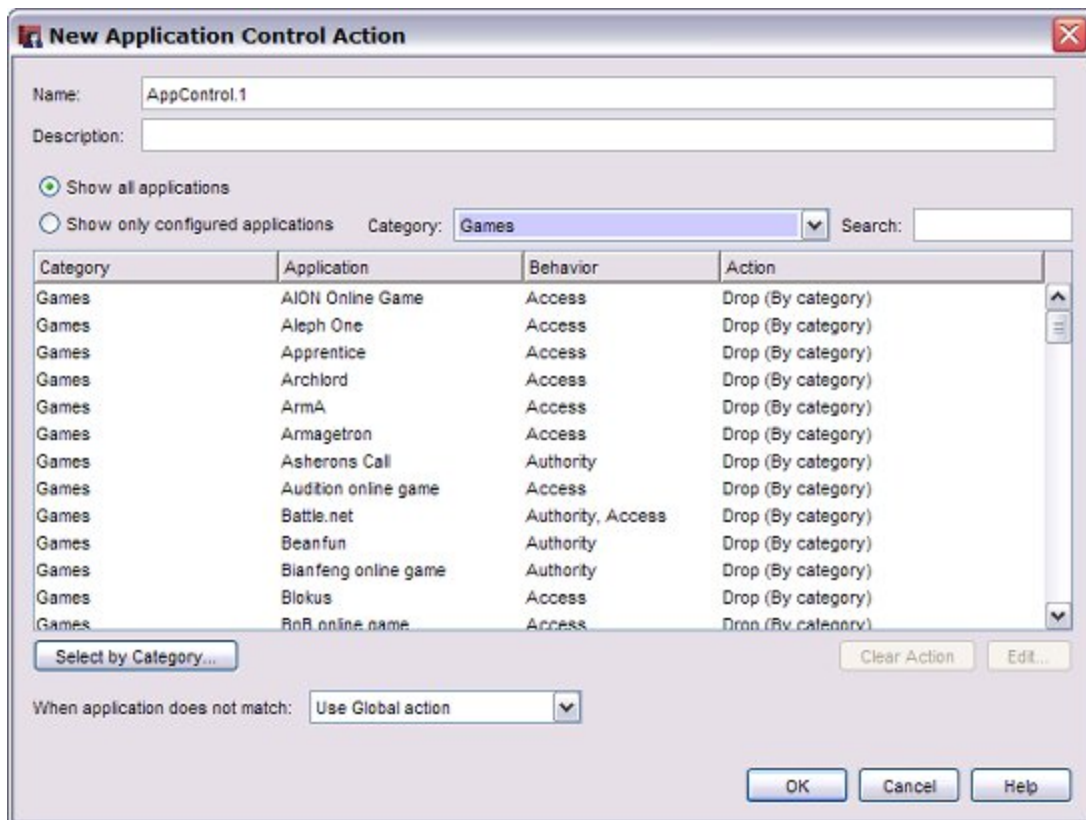
Application Categories are used to classify applications in Application Control reports. Categories also provide a convenient way to search for, or block, all applications in a category. To conveniently restrict the use of a set of applications that do not have legitimate business value, you can block all applications in a category. A good example is the **Games** application category.

To block all applications in the **Games** category for an Application Control action:

1. In the **Application Control Action** dialog box, click **Select by Category**.  
*The Select by Category dialog box appears.*



2. Select the **Games** check box.
3. From the **Games** drop-down list, select **Drop**.
4. Click **OK**.  
*All applications in the Games category have the action set to Drop (By category).*
5. To see the blocked games, select **Games** from the **Category** drop-down list.



When any new applications are added to the **Games** category by the signature update process, they are also blocked by this Application Control action.

When an application action is configured based on a category action, the **Action** column shows the label (by category) after the configured action. You can still edit the action for a specific application in the category to override the category action, as described in the next section.

When you configure an action for an application category, any future applications that are added to the category are automatically configured to use the same category action.

If you configure Application Control to block all applications in a category, make sure you know everything that is included in the category and the expected consequences. For example, SWF (Shockwave Flash) is included in the streaming media category. Flash is used widely in many web sites to deliver content. If you block all streaming media, Flash content is also blocked.

We do not recommend that you configure Application Control to block general categories like Web / Web 2.0, Business, or Network Protocols. It is likely that this could block an application that you did not intend to block, or that has other, unintended consequences.

We recommend that you set up Application Control to send log messages for all activity for a period of time before you configure any actions that block applications. This enables you to determine which applications to block.

## Override a Category Action

If you configure an action for an application category, you can set a different action for a specific application in that category. If you assign an action to a specific application, that action overrides the action configured for the category.

To override an action for an application that is in a configured category:

1. In the **Application Control Action** dialog box, select an application.
2. Click **Edit**.  
*The Application Control Configuration dialog box appears.*
3. Select the action for the application.  
For more information, see [Configure Application Control Actions](#).
4. Click **OK**.  
*The application-specific action replaces the category action for that application.*

## Application Control and Proxies

---

There is some duplication of the functions available in the Application Control service and in the WatchGuard proxy policies. In general, the proxies perform different and more detailed inspection and provide more granular control over the type of content. For example with the HTTP proxy, you can

- Adjust timeout and length limits of HTTP requests and responses to prevent poor network performance, as well as several attacks
- Customize the deny message that users see when they try to connect to a web site blocked by the HTTP proxy
- Filter web content MIME types
- Block specified path patterns and URLs
- Deny cookies from specified web sites

Proxies are also used to provide Gateway AntiVirus, WebBlocker, and Reputation Enabled Defense services.

By default, the HTTP proxy action blocks the download of these content types:

- Java bytecode
- ZIP archives
- Windows EXE/DLL files
- Windows CAB archive

The Application Control feature does not override settings in the proxy policy configuration. For example, if you allow YouTube in Application Control, but the proxy policy is already configured with an action to block streaming video, YouTube videos are still blocked.

## Application Control and WebBlocker

---

If both WebBlocker and Application Control are configured in the same policy, and the traffic matches for a web site and application, the Application Control action might or might not trigger first. Which action triggers first depends on several factors, such as the number of packets required to identify the application, and how much time it takes to look up and return a category for the URL. Consider facebook.com. All access to facebook.com can be blocked in WebBlocker if the “personals and dating” category is blocked.

One advantage of WebBlocker is that it displays a specific warning message in the user’s browser when a site is blocked. If your company policy is to restrict all access to Facebook, it may be appropriate to block it in WebBlocker. You can either block the “personals and dating” category or add a WebBlocker exception. Application Control provides more granular control over applications and their associated subfunctions. With Application Control, it is possible to allow access to Facebook, but not allow access to Facebook Games.

## Manage SSL Applications

---

Many web-based applications are accessible through SSL (HTTPS), as well as through HTTP. Organizations offer encrypted SSL connections to provide more security to users. SSL encryption can also make applications more difficult for Application Control to detect. When you block applications that are accessible through SSL, you might also need to specifically block the SSL login for that application to make sure that you block all access to that application.

For example, when you select to block the application **Google-Finance**, this blocks Google’s financial applications. But it does not block Google Finance over SSL. To block that, you must also block the application **Google Authentication via SSL**. It is important to understand that, once you block Google Authentication over SSL, you lose control over the granularity of all Google SSL applications to block. For example, access to Google Docs and Gmail over SSL is also blocked.

Similar behavior occurs for some Microsoft and Yahoo applications when they are accessed over SSL. There are corresponding signatures for Authentication over SSL for Microsoft and Yahoo and many other applications in the Application Control application list. To granularly manage these types of applications, you might want to block Authentication over SSL. Then you can use the application signatures to granularly configure the applications that can be used over the http access that is allowed.

## Manage Applications that Use Multiple Protocols

---

Many applications today, especially instant messaging and peer-to-peer applications, use multiple protocols and techniques to transfer files. For example, there are many clients that use the BitTorrent protocol and other protocols to transfer files. To fully block applications that use multiple protocols, you must configure Application Control with a combination of actions.

For example, when you select the BitTorrent Series application in an Application Control action, Application Control uses a set of rules that identify the BitTorrent protocol for peer-to-peer file sharing. Many different applications use BitTorrent as a method to download files. It is important to understand that if you configure Application Control to block BitTorrent Series, Application Control blocks BitTorrent use by all applications. There is no way to block BitTorrent use by one application, but allow it for other applications.

For more information, and a list of applications that use multiple protocols, see the Firewall XTM User Guide or Help.

## Monitor Downloads and File Transfers

---

Application Control includes two general purpose applications in the **File Transfer** category called **Web File Transfer** and **FTP Applications** that you can use to record log messages for common download and file transfer activity.

### *Web File Transfer*

Web File Transfer is a general application that detects the download of common file formats that are often downloaded through popular P2P and File Transfer programs, including: bz2 ,doc , exe , gz, pdf, ppt, rar , rpm, tar, xls, zip, torrent, dll, manifest, xdap, deploy, xps, , xaml, application, mkv, and dat. It also covers HTTP upload of files.

### *FTP Applications*

FTP Applications is an application that detects a range of FTP commands —pass, list, eprt, epsv, create directory, delete directory, get (binary and ascii), put (binary and ascii), passive and active file transfer.

These applications are best used to generate log messages of activity. Consider the implications carefully before you decide to block these applications, or the general File Transfer category.

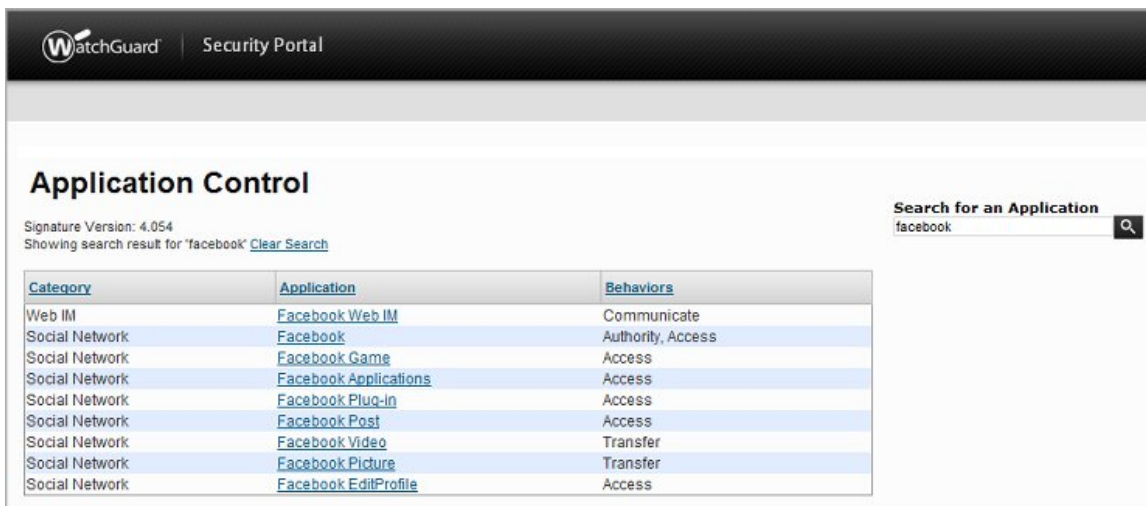
## Manage Facebook Applications

---

Some applications, such as Facebook, contain multiple application types that Application Control can identify. You can use Application Control to granularly control which applications your users can use.

Facebook is a social networking site that includes a large number of features and applications. You can use Application Control to block some or all Facebook applications. For example, you can configure an Application Control action that allows Facebook, but blocks the use of Facebook games or IM. Or you can block the use of all Facebook applications.

You can see the list of Facebook applications when you configure an Application Control action for your device, or you can search for *facebook* in the Application Control security portal at <http://www.watchguard.com/SecurityPortal/AppDB.aspx>.



Application Control can identify and block different types of Facebook activity.

*Facebook Web IM*

Identifies Facebook chat sessions.

*Facebook*

Identifies attempts to log in to Facebook or see Facebook web pages.

*Facebook Game*

Identifies the top 25 most popular Facebook games.

*Facebook Applications*

Identifies all applications available through the Facebook apps directory.

*Facebook Plug-in*

Identifies all Facebook social plug-ins that can be embedded in other sites on the Internet. This includes plug-ins such as **Like** and **Comments**. To see the current list of Facebook social plug-ins, see <http://developers.facebook.com/plugins>.

*Facebook Post*

Identifies information posts to Facebook. This includes:

- Post a message to the wall
- Share status
- Share a link

*Facebook Video*

Identifies video uploads to Facebook.

*Facebook Picture*

Identifies photo uploads to Facebook.

*Facebook EditProfile*

Identifies Facebook user profile updates.

To block Facebook applications:

1. Create or edit an Application Control action.
2. In the search text box, type `facebook`.  
*The list of applications is filtered to show only the Facebook applications.*
3. Select one or more Facebook applications to block.
4. Select **Edit**. Set the action for the selected applications to **Block**.
5. Apply the Application Control action to your policies.

## Application Control Policy Examples

---

You can use the **Global** Application Control action with other Application Control actions to allow or block different applications based on the time of day, or based on the user name or user group. To do this, you create Application Control actions that block or allow different sets of applications. Then you apply different Application Control actions to different policies as described in the examples below.

Each of the examples below enables Application Control actions for a single type of policy. If your configuration includes other policy types, such as TCP-UDP, or Outgoing, you can use the same steps to set up a two-tiered Application Control configuration for those policies. The policies you need to apply an Application Control action to depend on which policies exist in your configuration, and which applications you want to block. For example, if you want to block an application that you know uses FTP, you must enable the Application Control action for the FTP policy.

For recommendations on which types of policies to configure for Application Control, see [Policy Guidelines for Application Control](#).

### Allow an Application For a Group of Users

If the Global Application Control action blocks an application, you can create a separate Application Control action to allow that same application for a department or other user group. For example, if you want to block the use of MSN instant messaging for most users, but you want to allow this application for the people in the Sales department, you can create different Application Control actions and policies to get this result.

If you already have an **HTTP** packet filter policy that applies to all users, you can use these steps to allow different applications for the Sales department.

1. Configure the **Global** Application Control action to block MSN instant messaging, and any other applications you do not want to allow.
2. Apply the **Global** Application Control action to the existing **HTTP** packet filter policy.
3. Create a new Application Control action to allow MSN instant messaging. For example, you could call this action, **AllowIM**. Configure this action to use the **Global** action when the application does not match.
4. Create an HTTP policy for the users in the Sales department. For example, you could call this policy **HTTP-Sales**.
5. Apply the **AllowIM** Application Control action to the **HTTP-Sales** policy.
6. Enable logging for the **HTTP** and **HTTP-Sales** policies.

*You must enable logging to see information about Application Control in the log files and reports.*

In this example, the two resulting HTTP policies could look like this:

*Policy: HTTP-Sales*

HTTP connections are: **Allowed**  
From: **Sales** To: **Any-External**  
Application Control: **AllowIM**

*Policy: HTTP*

HTTP connections are: **Allowed**  
From: **Any-Trusted** To: **Any-External**  
Application Control: **Global**

The **AllowIM** Application Control action applied to the **HTTP-Sales** policy acts as an exception to the **Global** Application Control action. The users in the Sales group can use MSN instant messaging, but cannot use any other applications blocked by the **Global** Application Control action.

If this device configuration included other policies, such as HTTP-Proxy, TCP-UDP, or Outgoing, that could be used for IM traffic, you can repeat the steps above to set up a two-tiered Application Control configuration for other policies.

## Block Applications During Business Hours

You can use Application Control with policies to block different applications based on the time of day. For example, you might want to block the use of games during business hours. To block applications during certain hours, you can use Application Control with policies that have an operating schedule.

If you already have an **HTTP-Proxy** policy that does not have an operating schedule, use these steps to add a new policy and Application Control action to block applications during business hours.

1. Configure the **Global** Application Control action to block applications you want to always block.
2. Apply the **Global** Application Control action to the existing **HTTP-Proxy** policy.
3. Create a schedule called **Business-Hours** that defines the business hours.
4. Create a new HTTP-Proxy policy that uses the **Business-Hours** schedule you configured. For example, you could call the new policy **HTTP-Proxy-Business**.
5. Create an Application Control action that blocks the applications you want to block during business hours. For example, you could call this action **Business**.
6. Apply the **Business** Application Control action to the **HTTP-Proxy-Business** policy.
7. Enable logging for the **HTTP-Proxy** and **HTTP-Proxy-Business** policies.  
*You must enable logging to see information about Application Control in the log files and reports.*

In this example, the two resulting policies could look like this:

*Policy: HTTP-Proxy-Business*

HTTP connections are: **Allowed**  
From: **Sales** To: **Any-External**  
Application Control: **Business**

*Policy: HTTP-Proxy*

HTTP connections are: **Allowed**  
From: **Any-Trusted** To: **Any-External**  
Application Control: **Global**

The **Business** Application Control action in the **HTTP-Proxy-Business** policy blocks games only during business hours. All other applications in the **Global** Application Control action are blocked at all times of day.

If this device configuration included other policies, such as HTTP, TCP-UDP, or Outgoing, that might be used for games traffic, you can repeat the steps above to set up a two-tiered Application Control configuration for other policies.

## For More Information

---

This guide provides information to help you to get started with Application Control. For more detailed information about how to configure Application Control, see these documentation resources:

- [Fireware XTM WatchGuard System Manager Help](#)
- [Fireware XTM Web UI Help](#)
- *Fireware XTM WatchGuard System Manager User Guide*
- *Fireware XTM Web UI User Guide*
- [Knowledge Base](#)