Filter IP How to Guide

Contents

Overview

The Swivel Administration Console can be protected by allowing access to a defined IP or range of IP addresses. The administrative filter is included as part of the Swivel 3.2 software and all subsequent releases.

Prerequisites

Swivel 3.2 onwards

Swivel 3.1.x filter can be added

How to use the IP Filter

Configuration

Swivel Core File location

The filter configuration is controlled by two files found in the conf folder

filter.properties, Determines the way the filter behaves when access is denied or granted.

ranges.xml, is a list of IP ranges that can access the Admin Console.

These files are located in:

Swivel version 3.9.1 onwards, see Transient Data Storage, <path to .swivel>/conf

Earlier versions of Swivel <path to Tomcat>/webapps/pinsafe/WEB-INF/conf:

Swivel Applications File Location

Applications such as the Sivel Authentication manager will have their filter located under home/swivel/<application_name>/security.properies and is similar to the ranges.xml file.

Editing filter.properties

The default filter.properties file is shown below.

```
#
# Admin Console Filter Localization
#
# Commented lines will result in no message being logged
#
# ALLOWED = Access Allowed
DENIED = Access Denied
ERROR = Page Not Found
# FILTERING = Filtering
STATUS = 404
```

The entries are as follows:

ALLOWED Message written to TOMCAT console with request IP address when the filter allows access. When Commented out; filter is silent. Default: Commented out

DENIED Message written to TOMCAT console with request IP address when the filter denies access. Default: Access Denied

ERROR Message reported back to browser when access is denied. If not set, no response is sent and the browser will eventually time out. Default: Page Not Found

FILTERING Message written to TOMCAT console followed by address ranges as TOMCAT initializes the filter. When Commented out; filter is silent. Default: Commented out

STATUS The http status code reported back when access is denied. This should match the error message. Default: 404

Editing ranges.xml

The ranges.xml file holds the list of IP addresses that are allowed to access the admin console

The default ranges.xml file is shown below.

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
<properties>
       <entry key="anyone">0/0</entry>
       <entry key="anyone6">::0/0</entry>
       <entry key="localhost">127.0.0.1/255.255.255.255</entry>
       <entry key="localhost6">::1/128</entry>
</properties>
```

The default configured ranges.are named ?anyone? and ?localhost? and represent access from any IP address and localhost only respectively.

An address range is specified as an IP address followed (optionally) by a mask. The mask can be a single integer representing the number of significant address bits that must match for access to be allowed or it can be an IP-style dotted decimal. Both styles are present in the default file, but further examples are shown below.

The default entries allow access from all IP addresses. Removing the entry for ?anyone? will restrict access to localhost. Further ranges can be added to ease administration. All ranges should have a unique name.

IP Range Meaning

A /0 mask means that no bits need to match in the address. This allows access from all IP addresses.

Example 1:

0/0

123.123.123.123/0

A /32 mask means all 32 bits must match. The equivalent dotted-decimal is 255.255.255.255. Specifying no mask is the same as specifying a /32 mask.

Example 2:

127.0.0.1/32

127.0.0.1/255.255.255.255

127.0.0.1

To allow access from any address on the 192.168.0 subnet.

Example 3:

192.168.0.0/24

192.168.0.0/255.255.255.0

The values for <entry key="anyone6">::0/0</entry> and <entry key="localhost6">::1/128</entry> are for IPv6

Editing what is filtered

By default all access to the admin port is filtered. It is possible to define specific access using the filter. What is filtered is controlled by the web.xml file, this file is usually located as follows:

Appliance: /usr/local/tomcat/webapps/pinsafe/WEB-INF/web.xml

Software only: C:\Program Files\Apache Software Foundation\Tomcat 6.0\webapps\pinsafe\WEB-INF\web.xml

Look for the following entry:

```
<filter-mapping>
               <filter-name>adminConsoleFilter</filter-name>
               <url-pattern>/*</url-pattern>
       </filter-mapping>
```

To filter just the TURing image request, change this to:

```
<filter-mapping>
               <filter-name>adminConsoleFilter</filter-name>
               <url-pattern>/SCImage</url-pattern>
       </filter-mapping>
```

Activating the filter

Restart Tomcat

Testing

When someone attempts to access any part of the admin console they are redirected to the admin log-in page. At this point the filter intercepts the request and checks to see if the IP address is on the allowed list. If it is not allowed then a message will display **Swivel is running. Click here to open Swivel admin console.** but clicking on the link has no effect. Older versions return the error code and message defined in the filter.properties file.

Known Issues

Swivel version 3.10.4 increases the filtering and additional access may need to be added for Agents and other resources accessing Swivel.

More recent versions display **Swivel is running. Click here to open Swivel admin console.** instead of the messages in the filter.properties file.

Windows Server 2008 by default treats "localhost" as an IPv6 address (::1), rather than IPv4 (127.0.0.1), so if the ranges file doesn't include the IPv6 address, it will fail. The one that comes with Swivel 3.8 includes additional entries to cover IPv6 addresses.

If you have customised your ranges.xml, then you can try the following:

Connect to Swivel using 127.0.0.1 rather than localhost

Disable IPv6 on the server

Add the following entries to ranges.xml:

```
 ::1/128 (to allow localhost on IPv6)
```

```
 ::0/0 (to allow any address on IPv6)
```

Troubleshooting

Check the Tomcat logs, these are located under <path to Tomcat>/logs. The localhost.<date> log will contain failed connection attempts

INFO: Access Denied x.x.x.x