# Web Security Gateway

v8.5.x

## Content Gateway Troubleshooting

Revision A

Contents

- Dropped HTTPS connections on page 2
- Websites that have difficulty transiting Content Gateway on page 3
- Sites that host applications that don’t handle NTLM authentication on page 11
- Restricted users fail to authenticate with NTLM on page 12
- Content Gateway does not resolve websites on page 12
- Content Gateway command line commands do not execute on page 12
- Inconsistent behavior related to objects in the cluster on page 13
- Browser displays a data missing message on page 13
- DrainIncomingChannel message in the system log file on page 14
- Warning in system log file when editing vaddrs.config on page 14
- Explicit proxy requests fail after enabling always_query_destination on page 14
- Content Gateway is running but no log files are created on page 15

# Dropped HTTPS connections

Some application protocols that tunnel using port 443 may attempt to establish a connection with Content Gateway using a variant of HTTPS that Content Gateway doesn’t accept. When HTTPS is enabled in Content Gateway, these attempted connections are dropped by Content Gateway. Connections using QIP 2005 are an example of this type of application protocol.

When HTTPS is disabled, SSL connections don’t pass through Content Gateway and this type of connection is not an issue.

When HTTPS is enabled, the issue can be handled in either of two ways:

- Configure Content Gateway to tunnel unknown protocols.
- Add incidents to the Content Gateway SSL Incidents list to tunnel these application protocols.

## Tunneling unknown protocols

Content Gateway can be configured to tunnel all unknown protocols. However, because this option allows all traffic to tunnel through port 443, it seriously compromises network security.

To tunnel unknown protocols:

### Steps

1) Log on to the Content Gateway manager and go to **Configure** > **Protocols** > **HTTPS**.

2) Enable the **Tunnel Unknown Protocols** option, click **Apply** and restart Content Gateway.

## Adding SSL incidents

### Before you begin

You can add a URL to the SSL Incident list to allow Content Gateway to tunnel connections to specified HTTPS websites. This option has the advantage of easy configuration in the Content Gateway manager. However, it may be an impractical alternative if a very large number of URLs must be entered.

To add a website to the SSL Incident List:

### Steps

1) In Content Gateway manager, go to **Configure** > **SSL** > **Incidents** > **Add Website**.

2) In the **URL** field specify the URL that you want to tunnel.

3) Select **By URL** and for **Action** select **Tunnel**.

4) Click **Apply**.

# Websites that have difficulty transiting Content Gateway

This article lists sites and applications that do not work as expected with Content Gateway and offers appropriate PAC file entries, bypass rules, filtering rules, and other solutions to provide access to those resources.

**Important**

It is up to you to determine and apply the solution that is best for your deployment and security environment.

## Background

Because of the way some sites package content or use (or misuse) the HTTP/HTTPS protocols, those sites have difficulty transiting Content Gateway (and most other proxy servers).

When access to those sites is required, Content Gateway provides several ways to specify sites that will bypass the proxy, including static and dynamic bypass rules, and, when HTTPS is enabled, SSL Incident rules.

In addition, depending on how Content Gateway is deployed in the network, sites can be bypassed with a PAC file entry (explicit proxy deployments with most Windows clients), or via the Access Control List (ACL) on the router or switch (transparent proxy deployments).

In addition, sites that host applications that do not properly negotiate proxy user authentication are also a problem. When use of those applications is a requirement, it is possible to create a proxy filtering rule that identifies the application through the User-Agent field of the HTTP header and allows the application to bypass user authentication.

For more about bypass rules, see Interception Bypass in Content Gateway Manager Help.

For more about SSL incident rules, see Managing HTTPS website access in Content Gateway Manager Help.

For more about bypassing a site using a PAC file, see How do I specify in a PAC file a URL that will bypass Content Gateway?

See your router or switch documentation for information about ACLs.

# Default SSL bypass rules

When HTTPS (SSL support) is enabled for HTTPS decryption, inspection, and re-encryption, these Incident list entries are present and enabled by default:

| URL | Action | Purpose |
|---|---|---|
| *.microsoft.com:443 | default tunnel | Microsoft Update and Windows Update |
| *.msn.com:443 | default tunnel | Microsoft Update and Windows Update |
| *.gotomeeting.com:443 | default tunnel | Citrix GoToMeeting |
| *.webex.com:443 | default tunnel | Cisco collaboration tools |
| aus2.mozilla.org:443 | default tunnel | Firefox Update |
| *.blackspider.com:443 | default tunnel | Forcepoint Web Security Cloud connection |
| *.mailcontrol.com:443 | default tunnel | Forcepoint Email Security Cloud connection |
| *.citrixonline.com:443 | default tunnel | Citrix collaboration tools |
| *.expertcity.com:443 | default tunnel | Citrix collaboration tool support |
| *.gotoassist.com:443 | default tunnel | Citrix remote assistance tool |
| *.gofastchat.com:443 | default tunnel | Citrix collaboration tool support |
| *.gotomypc.com:443 | default tunnel | Citrix remote PC access tool |
| *.goview.com:443 | default tunnel | Citrix collaboration tool |

# Sites that have difficulty transiting Content Gateway

**Related concepts**

Real Networks Real Player on page 8

**Related tasks**

Logitech Messenger Agent and VirtualBox on page 10

**Related reference**

Microsoft Update on page 5
WebEx on page 6
Citrix collaboration products on page 9
Firefox Update on page 9
Yahoo! Messenger with Pidgin messaging client on page 10

# Microsoft Update

Microsoft Update updates the Windows operating system and Microsoft applications, such as Office. The update process runs as a system service and consequently does not use the same certificate trusts as a user.

**Note**

When Microsoft Update is accessed with HTTP, no special configuration is required. However, because the connection is not secure, this method is not recommended.

To use Microsoft Update with HTTPS when SSL support is enabled, you must bypass the proxy in one of the following ways:

| | |
|---|---|
| **PAC file entry:** | /* Don't proxy Microsoft Update */<br>if ((host == "download.microsoft.com") \|\| (host == "ntservicepack.microsoft.com") \|\| (host == "cdm.microsoft.com") \|\|<br>(host == "wustat.windows.com") \|\|<br>(host == "windowsupdate.microsoft.com") \|\| (dnsDomainIs(host, ".windowsupdate.microsoft.com")) \|\| (host == "update.microsoft.com") \|\|<br>(dnsDomainIs(host, ".update.microsoft.com")) \|\| (dnsDomainIs(host, ".windowsupdate.com")))<br>{<br>return 'DIRECT';<br>} |
| **Static bypass rule:** | Not recommended due to the number of IP address ranges used by Microsoft and the dynamic nature of that IP address set. |
| **SSL incident rule:** | The rules that are included in the Incident List by default are sufficient. |

Alternatively, you can disable Microsoft Update and use Windows Update instead. Windows Update only updates the operating system and doesn't have problems transiting the proxy.

If you elect to use Windows Update:

1) Add the URL to the **Scanning: Never Scan** list (in the Web Security module of Forcepoint Security Manager).

2) In the Content Gateway manager, go to **Configure** > **Protocols** > **HTTP** > **Timeouts**, and make sure that the **Keep-Alive Timeouts** value is set to **60**.

On Windows 7 systems, to repair Microsoft Windows error 80072F8F, navigate to **Start** > **Control Panel** > **Troubleshooter** > **System and Security** and select **Fix problem with Windows Update**.

# WebEx

WebEx does not support HTTPS connections through a proxy. Use one of the following bypass methods.

| | |
|---|---|
| **PAC file entry:** | if (shExpMatch(url, "*.webex.com/*"))<br>{<br>return "DIRECT";<br>} |
| **Static bypass rule:** | This method requires creation of several bypass rules, one for each current IP address range. For each IP address range: |
| | Rule Type: Bypass |
| | Source IP: (empty) |
| | Destination IP: <IP address range> |
| | The list of IP addresses for Cisco Unified MeetingPlace version 8.5 is: |
| | 64.68.96.0/19 (CIDR) or 64.68.96.0 - 64.68.127.255 (net range) |
| | 66.114.160.0/20 (CIDR) or 66.114.160.0 - 66.114.175.255 (net range) |
| | 66.163.32.0/20 (CIDR) or 66.163.32.0 - 66.163.47.255 (net range) |
| | 209.197.192.0/19 (CIDR) or 209.197.192.0 - 209.197.223.255 (net range) |
| | 208.8.81.0/24 (CIDR) or 208.8.81.0 - 208.8.81.255 (net range) |
| | 210.4.192.0/20 (CIDR) or 210.4.192.0 - 210.4.207.255 (net range) |
| | 62.109.192.0/18 (CIDR) or 62.109.192.0 - 62.109.255.255 (net range) |
| | 173.243.0.0/20 (CIDR) or 173.243.0.0 - 173.243.15.255 (net range) |
| | 114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range) |

| | |
|---|---|
| | More more information, see below. |
| **SSL incident rule:** | Add:<br>URL *.webex.com TUNNEL |

**Troubleshooting:** If after adding a bypass, the connection still fails, in some cases the WebEx site responds with an IP address or a domain name that doesn't match *.webex.com. You can work around the problem by examining the **inbound_access.log** to find the unresolved connection and then add the IP address or domain name as an exception using the option employed above.

> **Note**
>
> When Content Gateway is on an appliance, this procedure requires the assistance of Technical Support.

## Procedure to find the name of the WebEx site:

### Steps

1) On the Content Gateway host, change directory to /opt/WCG/sxsuite/log and open or view **inbound_access.log**.

2) Most often, the unresolved CONNECT will be in close proximity to a successful *.webex.com connect, so start by searching for webex.com. A successful tunnel connection looks similar to:

   ```
   CONNECT cisco.webex.com:443 HTTP/1.0
   CONNECT nsj1msccl01.webex.com:443 HTTP/1.1
   (tunneled SSL connection to nsj1msccl01.webex.com:443)
   (tunneled SSL connection to cisco.webex.com:443)
   ```

3) From this location scan downward for a URL that has the CONNECT status, but does not indicate that the connect was tunneled or successfully fetched content with a GET. This unresolved traffic might look similar to:

   ```
   CONNECT 66.114.169.162:443 HTTP/1.1
   CONNECT 66.114.169.162:443 HTTP/1.1
   ```

4) Add the domain name or IP address to the incident list or bypass list.

# WebEx domain, IP addresses, and ports (19-Feb-2013):

World Wide URL domain exception = *.webex.com

IP addresses and ranges:

- 64.68.96.0/19 (CIDR) or 64.68.96.0 - 64.68.127.255 (net range)
- 66.114.160.0/20 (CIDR) or 66.114.160.0 - 66.114.175.255 (net range)
- 66.163.32.0/20 (CIDR) or 66.163.32.0 - 66.163.47.255 (net range)
- 209.197.192.0/19 (CIDR) or 209.197.192.0 - 209.197.223.255 (net range)

- 208.8.81.0/24 (CIDR) or 208.8.81.0 - 208.8.81.255 (net range)
- 210.4.192.0/20 (CIDR) or 210.4.192.0 - 210.4.207.255 (net range)
- 62.109.192.0/18 (CIDR) or 62.109.192.0 - 62.109.255.255 (net range)
- 173.243.0.0/20 (CIDR) or 173.243.0.0 - 173.243.15.255 (net range)
- 114.29.192.0/19 (CIDR) or 114.29.192.0 - 114.29.223.255 (net range)

Ports that need to be open to clients (Internet):

| | | |
|---|---|---|
| TCP | 80 | Client Access |
| TCP | 443 | Client Access |
| TCP | 8554 | Audio Streaming Client Access |
| TCP/UDP | 53 | DNS |
| UDP | 7500 | Audio Streaming |
| UDP | 7501 | Audio Streaming |
| UDP | 9000 | VOIP/Video |
| UDP | 9001 | VOIP/Video |

# Real Networks Real Player

When the following **combined conditions are true**, Real Networks Real Player fails to stream content:

1) Content Gateway is deployed as an explicit proxy.

2) Content Gateway is the only path to the Internet.

3) User authentication is NTLM.

By default, Real Player uses the RTSP or PNA protocols to stream media, both of which bypass Content Gateway. However, when Content Gateway is the only path to the Internet, Real Player uses HTTP to transit Content Gateway. Unfortunately, Real Player doesn't handle NTLM authentication properly and the connection fails.

## Procedure to work around the problem

To work around the problem, add an **Allow** rule to **filter.config** that identifies the Real Player application and allows Real Player traffic to bypass authentication:

### Steps

1) In the Content Gateway manager, go to **Configure** > **Security** > **Access Control** > **Filtering** and click **Edit File**.

2) Add the following filtering rule:

   Rule Type = Allow<br>
   Primary Destination Type = dest_domain<br>
   Primary Destination Value = .<br>
   User-Agent = realplayer

3) Click **Add**. The new rule appears in the table at the top of the page. It should have the format:
Rule Type=Allow , dest_domain=. , User-Agent=realplayer

4) Click **Apply** and then **Close**.

# Citrix collaboration products

Citrix collaboration products do not support HTTPS connections through a proxy. Connections require proxy bypass rules.

To create proxy bypass rules, you will need a list of the current Citrix URL ranges. Go to these sites for additional information.

- Optimal Firewall Configuration
- Whitelisting and LogMeIn

If Content Gateway is a transparent proxy with WCCP routers or switches, add the Citrix IP address ranges to the WCCP Access Control List (ACL).

| | |
|---|---|
| **PAC file entry:** | Add entries for the Citrix URLs in the exceptions block of your PAC file. A separate line is required for each distinct IP address range.<br>if (shExpMatch(url, "Citrix Collaboration IP address"))<br>{<br>return "DIRECT";<br>}<br>where "Citrix Collaboration IP address" is replaced by an IP address range from the Citrix list. |
| **Static** | For each Citrix IP address range, add a rule like: |
| **bypass rule:** | |
| | Rule Type: bypass |
| | Source IP: (empty) |
| | Destination IP: IP address range or CIDR of one of the Citrix ranges |
| | Repeat for each range. |

# Firefox Update

The Firefox Update site does not support HTTPS connections through a proxy.

| | |
|---|---|
| **PAC file entry:** | if (shExpMatch(url, aus2.mozilla.org))<br>{<br>return "DIRECT";<br>} |

| | |
|---|---|
| **Static bypass rule:** | Add:<br>Rule Type: Bypass Source IP: (empty)<br>Destination IP: IP address range of Firefox Update |
| **SSL incident rule:** | Add:<br>URL aus2.mozilla.org TUNNEL |

# Yahoo! Messenger with Pidgin messaging client

When the Pidgin messaging client is used with Yahoo! Messenger, the SSL connection is blocked. Traffic can be permitted by adding one or two rules to the SSL Incident list.

The message traffic cannot be meaningfully scanned, therefore it is recommended that you add the URL to the **Scanning: Never Scan** list (in the Web Security module of Forcepoint Security Manager).

| | |
|---|---|
| **PAC file entry:** | if (shExpMatch(url, scsa.msg.yahoo.com)) \|\| (shExpMatch(url, filetransfer.msg.yahoo.com))<br>{<br>return "DIRECT";<br>}<br>To prevent file transfers, remove “filetransfer.msg.yahoo.com” from the above code. |
| **SSL incident rule:** | Add:<br>URL scsa.msg.yahoo.comTUNNEL<br>URL filetransfer.msg.yahoo.com TUNNEL<br>Or, to block filetransfers, make the filetransfer rule BLACKLIST. |

# Logitech Messenger Agent and VirtualBox

These sites do not handle proxy NTLM authentication and require a **filter.config** authentication bypass rule.

## Steps

1) In Content Gateway Manager, go to **Configure** > **Security** > **Access Control** > **Filtering** and click **Edit File**.

2) Add the following filtering rule:
   Rule Type = Allow

   Primary Destination Type = dest_domain

   Primary Destination Value = (enter the appropriate value)

   .logitech.com

   .virtualbox.org

3) Click **Add**. The new rule appears in the table at the top of the page. It should have the format:
   Rule Type=Allow , dest_domain=value-you-entered

4) Click **Apply** and then **Close**.

# Sites that host applications that don’t handle NTLM authentication

## Before you begin

When Content Gateway is configured to perform NTLM authentication, some websites still challenge for credentials. This happens when the site hosts an application that is trying to start, but which fails to complete NTLM authentication. This is usually because the application is attempting some non-standard NTLM communication.

If manual authentication is unacceptable, you can create an **allow rule** in **filter.config** for each site that hosts an application that doesn’t know how to authenticate. This rule allows the application to bypass authentication.

For example:

## Steps

1) In the Content Gateway manager, go to **Configure** > **Security** > **Access Control** > **Filtering**.

2) Click **Edit File**.

3) Add a rule:

```
Rule Type=allow, dest_domain=example.com
```

4) Click **Apply** and **Close**.

5) On the Linux command line, in `/opt/WCG/bin` (substitute your Content Gateway installation location), run:

```
content_line -x
```

## Next steps

For more information, see the sections titled “Controlling access to websites” and “filter.config” in Content Gateway manager Help.

# Restricted users fail to authenticate with NTLM

When Content Gateway is configured to perform Legacy NTLM authentication with Active Directory, users who are restricted to a subset of workstations may not successfully authenticate.

The problem is due to the way Content Gateway establishes a session with the domain controller.

To work around the problem, in your Active Directory add a workstation named “TMP” and include it in the set of workstations available to the restricted users. TMP is the surrogate workstation name used by Content Gateway when establishing a session. TMP is used because, for security reasons, the actual workstation name is not provided by the browser in the authentication handshake.

# Content Gateway does not resolve websites

The browser indicates that it is contacting the host and then times out with the following message:

*The document contains no data; Try again later, or contact the server's Administrator....*

Make sure that the system is configured correctly and that Content Gateway can read the name resolution file.

- Use the **nslookup** command to confirm that the server can resolve DNS lookups. For example:
  `nslookup www.example.com`
- Confirm that `/etc/resolv.conf` contains the valid IP address of your DNS server(s).
- On some systems, if the `/etc/resolv.conf` file is unreadable or has no name server entry, the operating system will use localhost as a name server. However, Content Gateway does not use this convention. If you want to use localhost as a name server, you must add a name server entry for 127.0.0.1 or 0.0.0.0 in `/etc/resolv.conf`.

> **Important**
>
> If the IP addresses in `/etc/resolv.conf` change, Content Gateway must be restarted.

# Content Gateway command line commands do not execute

Command line commands do not execute if:

- The **content_manager** process is not running.
  Confirm that the **content_manager** process is running by entering the following command:

  ```
  ps aux | grep content_manager
  ```

  or, from the `/opt/WCG` directory:

  ```
  ./WCGAdmin status
  ```

If the **content_manager** process is not running, to start it enter the following command from the Content Gateway bin directory (`/opt/WCG/bin`):

```
./content_manager
```

**Important**

If you must stop Content Gateway use:

```
./WCGAdmin stop
```

To start Content Gateway use:

```
./WCGAdmin start
```

To restart Content Gateway use:

```
./WCGAdmin restart
```

- You are not executing the command from $WCGHome/bin.
  If the Content Gateway bin directory is not in your path, make your working directory `/opt/WCG/bin` and prepend each command with './'

  For example:

  ```
  ./content_line -h
  ```

# Inconsistent behavior related to objects in the cluster

This is most likely a clock synchronization problem among nodes in the cluster. Minor time differences of a couple minutes should not cause problems, however larger discrepancies can affect Content Gateway operation.

It is recommended that you run a clock synchronization daemon such as **xntpd**. You can obtain the latest version of xntpd here: http://www.ntp.org

# Browser displays a data missing message

A browser displays a message similar to:

*Data Missing*

*This document resulted from a POST operation and has expired from the cache. If you wish you can repost the form data to re-create the document by pressing the reload button.*

Browsers maintain their local cache in memory on the client system. Browser messages about documents that have expired from cache examine the local cache, not the Content Gateway cache. There is no Content Gateway message or condition that can cause such a message to display.

For information about browser cache options and effects, see the browser documentation.

# DrainIncomingChannel message in the system log file

The following messages appear in the system log file:

*Feb 20 23:53:40 louis content_manager[4414]: ERROR ==> [drainIncomingChannel] Unknown message: 'GET http:// www.telechamada.pt/ HTTP/1.0'*

*Feb 20 23:53:46 louis last message repeated 1 time*

*Feb 20 23:53:58 louis content_manager[4414]: ERROR ==> [drainIncomingChannel] Unknown message: 'GET http:// www.ip.pt/ HTTP/1.0'*

These error messages indicate that a browser is sending HTTP requests to one of the Content Gateway cluster ports, either **rsport** (default port 8087) or **mcport** (default port 8088). Content Gateway discards the request. This error does not cause any Content Gateway problems. The browser must be reconfigured to use the correct proxy port.

⚠ **Important**

Content Gateway clusters work best when configured to use a separate network interface and cluster on a private subnet so that client machines have no access to the cluster ports.

# Warning in system log file when editing vaddrs.config

If you edit the **vaddrs.config** file as a non-root user, Content Gateway places a warning message in the system log file similar to:

*WARNING: interface is ignored: Operation not permitted.*

The message can be ignored. Content Gateway applies your configuration edits.

❗ **Warning**

You should always configure virtual IP addresses in the Content Gateway manager. Editing **vaddrs.config** directly can have unpredictable results.

# Explicit proxy requests fail after enabling always_query_destination

When requests are routed to Content Gateway in transparent proxy mode, the **records.config** variable **proxy.config.arm.always_query_dest** can be used to configure Content Gateway to ignore host headers and always ask for the IP address of the origin server. When this variable is enabled, Content Gateway obtains the origin server’s IP address from the inbound packet rather than trying to resolve the destination host name with a DNS lookup. As a result, logged URLs contain only IP addresses, not host names. To log domain names, you must disable **proxy.config.arm.always_query_dest** (set it to 0).

Explicit requests (non-transparent requests, including requests on port 80) fail, because there is no matching map in the NAT list.

> **Important**
>
> **always_query_destination** works only on the primary proxy port.

# Content Gateway is running but no log files are created

Content Gateway writes event log files only when there is information to record.

- If Content Gateway is idle, there may be no log files.
- Confirm that you are looking in the correct directory.
  By default, Content Gateway creates log files in its logs directory. Check the location of the log files in the Content Gateway manager by examining the Log Directory field on the **Configure** > **Subsystems** > **Logging** > **General** tab.
- Check that the log directory has read/write permissions for the Content Gateway user account. If the log directory does not have the correct permissions, the content_gateway process is unable to open or create log files.
- Check that logging is enabled. In the Content Gateway manager, examine the Logging area on the **Configure** > **Subsystems** > **Logging** > **General** tab.
- Check that a log format is enabled. In the Content Gateway manager, check that a standard format is enabled on the **Configure** > **Subsystems** > **Logging** > **Formats** tab or that the custom format is enabled on the **Custom** tab.

Published 02 September 2024