Troubleshooting DataCollection Web Service Install 404 Error

Megan De Freitas - 2024-11-22 - Miscellaneous

If you receive a 404 error in DataCollection, this does not always mean the file is missing. If you are sure the files are stored in the correct location and all settings are correct, please refer to the information below from Microsoft:

HTTP 404.x-File or Directory Not Found (IIS 6.0)

An HTTP 404 error indicates that the requested resource was not found. Table 11.8 HTTP 404 Substatus Codes lists the substatus codes for the 404 error. The descriptions for most substatus codes are self-explanatory. When additional information about a substatus code is required, it is provided in one of the following sections.

Table 11.8 HTTP 404 Substatus Codes

404 Substatus Code	Condition
None	File or directory not found.
1	Web site not accessible on the requested port.
2	Web service extension lockdown policy prevents this request.
3	MIME map policy prevents this request.

Whether the requested resource is a file or a directory, begin by checking the following potential causes:

- Verify the file or directory. Examine the requested URL and check the physical path to which it maps.
- Check for unexpected host header routing. Problems with host headers occur when you have created more than one virtual Web server and rely on host header routing to serve content from the appropriate server. A 404 error results when you request a URL that exists on only one virtual server and, because of the configuration of the host header, the request is routed to the other virtual server.
- Verify that the request has been made on the correct port. The 404.1 error is returned when a request is made to a port on which the WWW service is not

listening.

- Ensure that the requested file is not hidden. IIS sends a 404 error if the Hidden file attribute for a requested file is set.
- Validate (*ScriptMaps) Web service extension requests. 404 errors are sometimes returned when you have a *ScriptMap Web service extension and the *Verify that file exists* option is set to True. If no file is actually associated with a *ScriptMap request, IIS cannot check for the file, so it returns a 404 error.

Both the Web service extension lockdown policy and MimeMap restriction features can cause a 404 error to be returned to the client making the request. If one of these features is the cause of an HTTP 404 error, do the following:

- Check the sc-substatus field for the request in the IIS W3C extended log. For information about enabling substatus logging, see Using Substatus and Win32 Errors in W3C Extended Logging.
- Check the Win32 error in the IIS W3C extended log. By default, IIS logs all Win32 errors associated with the request that are returned by the underlying operating system.
- Enable a modified custom error for the HTTP 404 error that you suspect. You can configure IIS to return a response to the client that contains the substatus code by editing the custom error page for the 404 error, and placing some custom text into the file. The custom error pages are located in *systemroot*\Help\IisHelp\Common.

Important: Enabling a custom error that provides substatus information undermines the security strategy used by IIS and should be done temporarily and only for troubleshooting purposes.

404.1-Web Site Not Accessible on the Requested Port

The 404.1 error can occur only on computers with multiple IP addresses. If a specific IP address/port combination receives a client request, and the IP address is not configured to listen on that particular port, IIS returns a 404.1 HTTP error.

For example, if a computer has two IP addresses and only one of those IP addresses is configured to listen on port 80, any requests received on the other IP address with port 80 causes IIS to return a 404.1 error. This error should be set only at the service level because it is returned to clients only when multiple IP addresses are used on the server.

404.2-Lockdown Policy Prevents This Request

If a request is denied because the associated ISAPI or CGI has not been unlocked, a 404.2 error is returned. When substatus logging is enabled, if you look at this request in the IIS logs, you will see an entry similar to the following:

2002-11-25 05:46:15 127.0.0.1 GET /default.asp - 80 - 127.0.0.1 - 404 2 1260

If IIS logging is not configured to log the substatus code, you can check the Win32 error to verify this condition. When a 404.2 error occurs, IIS logs the Win32 error 1260, which is an

ERROR_ACCESS_DISABLED_BY_POLICY error.

404.3-MIME Map Policy Prevents This Request

If a request is denied because a MIME map restriction is in effect, a 404.3 error is returned. When substatus logging is enabled, if you look at this request in the IIS logs, you will see an entry similar to the following:

2002-11-25 05:46:27 127.0.0.1 GET /somefile.unkext - 80 - 127.0.0.1 - 404 3 50

As with a 404.2 error, a 404.3 error causes a Win32 error to be logged. In this case, the error is 50, which is an ERROR_NOT_SUPPORTED error.

Another quick way to verify that a MIME map restriction is in effect is to add a wildcard MIME type to the virtual directory in question. This enables all MIME types to be served without restriction. Then, repeat the failed HTTP request and verify that it is served successfully.

Note: Adding a wildcard MIME type to the virtual directory is a troubleshooting step, not a solution to the problem. Leaving the wildcard in place and allowing all MIME types to be served compromises the security of the server.

For more information about adding a wildcard MIME type, see Working with MIME Types.

405-HTTP Verb Used to Access This Page Is Not Allowed

This HTTP code is returned when the client makes an HTTP request that contains a verb that is not allowed. This condition can occur when:

- A request for static content contains verbs other than GET or HEAD, and the request is made to a URL that did not end with a /. Instead performing a courtesy redirect, IIS sends the 405 error.
- An HTTP request for an ISAPI application contains a verb not listed in the ScriptMaps configuration for that ISAPI.

407-Initial Proxy Authentication Required by the Web Server

This error indicates that an intermediary proxy server between the HTTP client and the Web server requires some form of authentication. How you troubleshoot this kind of error depends upon the proxy server itself. Generally speaking, running a network trace with Network Monitor is helpful. If the Web client is a custom client, ask its developer to ensure that it is handling security appropriately.

413-Request Entity Is Too Large

For security reasons, you can limit the size of the *entity-body* of an HTTP request by modifying the MaxRequestEntityAllowed metabase property. When an entity-body of a client request exceeds the size that is specified in the MaxRequestEntityAllowed property, IIS returns a 413 error. If this error is logged for an individual request, an application on the Web server might have encountered an unexpected event and generated a request that is too large. If this error is logged for many requests, a malicious user might be attempting to compromise your Web server.

414-Request URL Is Too Large and Therefore Unacceptable on the Web Server

Just as the entity body of a request can be too large for IIS to process, a URL can be too long for IIS to process. IIS returns a 414 error if this occurs.

Miscellaneous

1. The DataCollection web service setup file (MSI) needs to be executed from an elevated command prompt in Windows Server 2012. MSI files do not have the ability to run as an administrator by right-clicking. The installer will fail if not run with elevated privileges.
2. The AppPoolIdentity may need to be updated for the default app pool. A network service account may need to be used in order for the web service to work properly.
3. Read/write privileges need to be granted to IIS users for the c:\windows\temp directory.