

Re: Windows Update v5 issues and workaround

Source: <http://www.tech-archive.net/Archive/ISA/microsoft.public.isa.clients/2004-09/0017.html>

From: Jim Harrison [MSFT] (jmharr_at_online.microsoft.com)

Date: 09/08/04

Date: Tue, 7 Sep 2004 19:46:02 -0700

No, you're not forgotten.

The WU team is hard at it coming up with an answer to this issue.

We've also tested a few more scenarios and here is an updated workaround for SIA 200x:

Synopsis:

There are two NTLM authentication issues affecting WU v5 when WU uses web proxy requests to access Windows Update:

- NTLMSSP_AUTH responses may contain null credentials

- NTLMSSP_NEGOTIATE credentials may be sent on a half-closed connection

We haven't heard any reports of WUv5 issues with non-NTLM (Basic, Digest) authentication yet and we haven't specifically tested

this.

We have been able to repro this with ISA Server 2000 and we have also heard reports of WU failing through other NTLM-authenticating

proxy servers (Proxy 2, Squid are two examples).

The cause of each problem is still being worked out, but a clear workaround is available and it boils down to two things:

- Disable authentication for Windows Update requests.
- Disable authentication for HTTP and HTTPS protocols

ISA Server Note: you may have heard that the "ReturnDeniedIfAuthenticated registry setting explained in <http://support.microsoft.com/?id=297324> is part of the problem. While applying this setting to ISA 2000 does help expose the WU

authentication problems, it is not the cause. If you have applied this setting to your ISA 2000 Server, you did so with good reason

to solve a specific problem. You should not remove this setting if you have applied it. By the same token, if you are not

experiencing the problem outlined in this KB article, you don't need to and shouldn't apply it. The above article applies only to

ISA 2000; you should not apply any ISA 2000 registry settings to ISA 2004 unless the relevant KB article explicitly instructs you

to. Currently, none do.

Now let's get on with the workaround.

Per the WU team, there are four destinations that should be included for creating anonymous Windows Update access policies:

TABLE 1

Item FQDN

- 1 *.download.microsoft.com
- 2 *.windowupdate.com
- 3 *.windowsupdate.microsoft.com
- 4 windowsupdate.microsoft.com

For internal clients

Download and apply this Internet Explorer update package to all internal clients

<http://support.microsoft.com/?id=871260>

For ISA 2000

NOTE: Changes to ISA 2000 policies do not take effect immediately and do not affect existing sessions.

See

<http://support.microsoft.com/?id=281985> for details.

Create a destination set for Windows Update domains

1. Expand <ArrayName> and PolicyElements
2. R-click Destination Sets, select New, then Set
3. Enter WindowsUpdate in the Name field, click Next
4. Click Add
5. Enter *.download.microsoft.com in the Domain field
6. Leave the Path field blank
7. Click OK
8. Repeat steps 4 through 7 for each remaining entry in Table 1
9. Click OK

Create an anonymous Site and Content rule for Windows Update requests

1. Expand Access Policy
2. R-click Site and Content Rules, select New, then Rule
3. Enter Windows Update in the Name field, click Next
4. Select Allow, click Next
5. Select Allow access based on destination, click Next
6. In the Apply this rule to: drop-down list, select Specified Destination Set
7. In the Name: drop-down list, select Windows Update
8. Click Next, then Finish

NOTE: if your existing protocol rules require authentication (user or group-limited), you'll have to create an anonymous

protocol rule for HTTP and HTTPS as follows:

Create an anonymous Protocol rule for HTTP and HTTPS

1. Right click Protocol Rules, select New, then Rule
2. Enter Windows Update in the Name field, click Next
3. Select Allow, click Next
4. In the Apply this rule to: drop-down list, select Selected protocols
5. In the Protocols list, select HTTP and HTTPS, click Next
6. Click Next, Next, then Finish

For ISA 2004

NOTE: Changes to ISA 2004 policies do not affect existing sessions. See

<http://support.microsoft.com/?id=841140> for details.

Create an anonymous Access Rule for Windows Update

1. In the left pane, R-click Firewall Policy and select New, then Access Rule
2. Enter Windows Update in the Name field, click Next
3. Select Allow, click Next
4. In the This rule applies to: drop-down list, select Selected Protocols
5. Click Add
6. In the Add Protocols dialog, expand Web
7. Select HTTP and click Add
8. Select HTTPS and click Add
9. Click Close, then Next
10. In the Access Rule Sources dialog, click Add
11. In the Add Network Entities dialog, expand Networks
12. Select Internal and click Add
13. For each network where clients may request access to Windows Update, select that network object and click Add
14. Click Close, then Next
15. In the Access Rule Destinations window, click Add
16. In the Add Network Entities window menu bar, click New, then Domain Name Set
17. In the New Domain Name Set Policy Element window, enter Windows Update in the Name field
18. Click New
19. In the Domain names included in this set list, change the new entry to *.download.microsoft.com
20. Repeat steps 19 and 20 for each remaining entry in Table 1
21. Click OK
22. In the New Domain Name Set Policy Element window, select Windows Update, click Add, then Close
23. Click Next, Next, then Finish
24. In the top part of the middle pane, Apply and Discard buttons will appear; click Apply
25. When Apply New Configuration dialog reports "Changes to the configuration were successfully applied", click OK

Make the Windows Update rule the first rule

NOTE: If you prefer to list all of your deny rules first, then you can make the Window Update rule the first rule following them

1. In the left pane, select Firewall Policy
2. If Windows Update is already the first rule in the list, stop here
3. In the middle pane, select Windows Update
4. In the right pane select the Tasks tab
5. Click Move the selected rule up until Windows Update is the first rule in the list
6. In the top part of the middle pane, Apply and Discard buttons should appear; click Apply
7. When Apply New Configuration dialog reports "Changes to the configuration were successfully applied", click OK

Look for a KB that details the WU side of the issue and cross-links to an ISA KB with these instructions.

--

Jim Harrison [ISASE]

Read the help, books and articles!

This posting is provided "AS IS" with no warranties, and confers no rights.

"Jim Harrison [MSFT]" <jmharr@online.microsoft.com> wrote in message news:upKw7PD1EHA.748@TK2MSFT

Hi all,

We've located an existing fix that appears to alleviate WU issue #2:

<http://support.microsoft.com/?id=871260>

Accordingly, the previous instructions are amended as follows (if you previously had "global auth reason to enable it):

microsoft.public.isa.clients: Re: Windows Update v5 issues and workaround

(add)

For internal clients

Download and apply this Internet Explorer update package to all internal clients

<http://support.microsoft.com/?id=871260>

For ISA 2000

(add)

Note for ISA policy recommendations: If you use an "allow all destinations for selected user" recommendation may not work as expected because of the way ISA 2000 matches requests to rules.

a "rule order" in ISA 2000, you may wish to modify your "allow all destinations for selected user" Update for all users"

(delete)

Disable "global" authentication for web proxy requests

For ISA 2004

(delete)

Disable "global" authentication for web proxy requests

--

Jim Harrison [ISASE]

Read the help, books and articles!

This posting is provided "AS IS" with no warranties, and confers no rights.

"Jim Harrison [MSFT]" <jmharr@online.microsoft.com> wrote in message news:eoUhAmskEHA.1152@TK2MSF

Hello everyone,

The core cause of this problem is still being worked out, but a clear workaround is available and

- Disable authentication for Windows Update requests.

- Disable "global authentication" for web proxy requests

Note: you may have heard that the "ReturnDeniedIfAuthenticated registry setting explained in <http://support.microsoft.com/?id=871260> is part of the problem. While applying this setting to ISA 2000 does help expose the WU authentication

cause. If you have applied this setting to your ISA 2000 Server, you did so with good reason to stop

not remove this setting if you have applied it. By the same token, if you are not experiencing the

article, you don't need to and shouldn't apply it. The above article applies only to ISA 2000; you

registry settings to ISA 2004 unless the relevant KB article explicitly instructs you to. Current

Now let's get on with the workaround.

Per the WU team, there are four destinations that should be included for creating anonymous Windows

TABLE 1

Item	FQDN
------	------

1	*.download.microsoft.com
---	--------------------------

2	*.windowsupdate.com
---	---------------------

3	*.windowsupdate.microsoft.com
---	-------------------------------

4	windowsupdate.microsoft.com
---	-----------------------------

For ISA 2000

Disable "global" authentication for web proxy requests

1. Open the ISA Management MMC

2. Select View, then Advanced

3. Expand Servers and Arrays

4. R-click <ArrayName>, select Properties

5. Select Outgoing Web Requests

6. Uncheck Ask Unauthenticated users for identification

7. Click Apply,

8. When prompted, select Save the changes and restart the service(s)

9. Click OK

Create a destination set for Windows Update domains

1. Expand <ArrayName> and PolicyElements

2. R-click Destination Sets, select New, then Set

3. Enter WindowsUpdate in the Name field, click Next

4. Click Add

5. Enter *.download.microsoft.com in the Domain field

6. Leave the Path field blank

7. Click OK

8. Repeat steps 4 through 7 for each remaining entry in Table 1

9. Click OK

Create an anonymous Site and Content rule for Windows Update requests

1. Expand Access Policy

2. R-click Site and Content Rules, select New, then Rule

microsoft.public.isa.clients: Re: Windows Update v5 issues and workaround

3. Enter Windows Update in the Name field, click Next
4. Select Allow, click Next
5. Select Allow access based on destination, click Next
6. In the Apply this rule to: drop-down list, select Specified Destination Set
7. In the Name: drop-down list, select Windows Update
8. Click Next, then Finish

For ISA 2004

Disable "global" authentication for web proxy requests

1. Open the ISA Mangement MMC
2. Expand <ArrayName>, then Configuration
3. Select Networks
4. In the middle pane, select the Networks tab
5. R-click Internal and select Properties
6. Select the Web Proxy tab
7. Click Authentication
8. In the Authentication window, uncheck Require all users to authenticate, click OK
9. Click Apply, then OK
10. Repeat steps 5 through 9 for each network object where you allow Web Proxy requests

Create an anonymous Access Rule for Windows Update

1. In the left pane, R-click Firewall Policy and select New, then Access Rule
2. Enter Windows Update in the Name field, click Next
3. Select Allow, click Next
4. In the This rule applies to: drop-down list, select Selected Protocols
5. Click Add
6. In the Add Protocols dialog, expand Web
7. Select HTTP and click Add
8. Select HTTPS and click Add
9. Click Close, then Next
10. In the Access Rule Sources dialog, click Add
11. In the Add Network Entities dialog, expand Networks
12. Select Internal and click Add
13. For each network where you unchecked Require all users to authenticate, select that network
14. Click Close, then Next
15. In the Access Rule Destinations window, click Add
16. In the Add Network Entities window menu bar, click New, then Domain Name Set
17. In the New Domain Name Set Policy Element window, enter Windows Update in the Name field
18. Click New
19. In the Domain names included in this set list, change the new entry to *.download.microsoft.com
20. Repeat steps 19 and 20 for each remaining entry in Table 1
21. Click OK
22. In the New Domain Name Set Policy Element window, select Windows Update, click Add, then Next
23. Click Next, Next, then Finish
24. In the top part of the middle pane, Apply and Discard buttons will appear; click Apply
25. When Apply New Configuration dialog reports "Changes to the configuration were successful"

Make the Windows Update rule the first rule

NOTE: If you prefer to list all of your deny rules first, then you can make the Window Update rule the first rule

1. In the left pane, select Firewall Policy
2. If Windows Update is already the first rule in the list, stop here
3. In the middle pane, select Windows Update
4. In the right pane select the Tasks tab
5. Click Move the selected rule up until Windows Update is the first rule in the list
6. In the top part of the middle pane, Apply and Discard buttons should appear; click Apply
7. When Apply New Configuration dialog reports "Changes to the configuration were successful"

Look for a WU KB soon that details the that side of the issue and cross-links to an ISA KB with the details

--

Jim Harrison [ISASE]

Read the help, books and articles!

This posting is provided "AS IS" with no warranties, and confers no rights.