

How to install KB15498768 – Current Branch 2207

In this post, I am going to install above KB to fix NTLM breach. Microsoft released the patch for CB2207 today. Please patch your production server ASAP.

KB15498768 covers the following issue:

NTLM connection fallback update for Microsoft Endpoint Configuration Manager

Article • 09/20/2022 • 2 minutes to read • 2 contributors



Applies to: Configuration Manager (current branch, versions 2103, 2107, 2111, 2203, 2207)

Summary of KB15498768

Disabling the **Allow connection fallback to NTLM** option in *Client Push Installation Properties* is not honored under either of the following conditions:

- If there are Kerberos authentication failures the client push account will attempt an NTLM connection instead.
- The site server computer account will attempt a connection using NTLM if Kerberos authentication fails for all defined client push installation accounts.

This update prevents any attempt at NTLM authentication for client push installation when the **Allow connection fallback to NTLM** option is disabled.

Installation of this update resolves the following security issue:

- [CVE-2022-37972](#)

Beginning with Configuration Manager current branch, version 2207, the **Allow connection fallback to NTLM** option is *disabled* by default on new site installations.

It is recommended to disable this option in existing environments, where possible, to increase security.

Refer to the following documents for more detail on client and NTLM security:

- [Security and privacy for Configuration Manager clients](#)
- [KB5005413: Mitigating NTLM Relay Attacks on Active Directory Certificate Services](#)
- [Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers](#)

Environments using versions of Configuration Manager current branch prior to 2103 are encouraged to update to a later supported version. Administrators can also disable use of automatic and manual client push installation methods to remove the risk of exposure to this issue. For more information, see [Support for Configuration Manager current branch versions](#).

Update information for Microsoft Endpoint Configuration Manager, versions 2103-2207

An update to resolve this issue is available in the **Updates and Servicing** node of the Configuration Manager console for environments that have versions 2103-2207 installed.

Update replacement information

This update does not replace any previously released updates.

Restart information

For Configuration Manager versions 2107 and later, this update does not require a computer restart or a [site reset](#) after installation.

Configuration Manager version 2103 will require a site reset after update installation.

Additional installation information

After you install this update on a primary site, pre-existing secondary sites must be manually updated. To update a secondary site in the Configuration Manager console, select **Administration > Site Configuration > Sites > Recover Secondary Site**, and then select the secondary site. The primary site then reinstalls that secondary site by using the updated files. Configurations and settings for the secondary site are not affected by this reinstallation. The new, upgraded, and reinstalled secondary sites under that primary site automatically receive this update.

Run the following SQL Server command on the site database to check whether the update version of a secondary site matches that of its parent primary site:

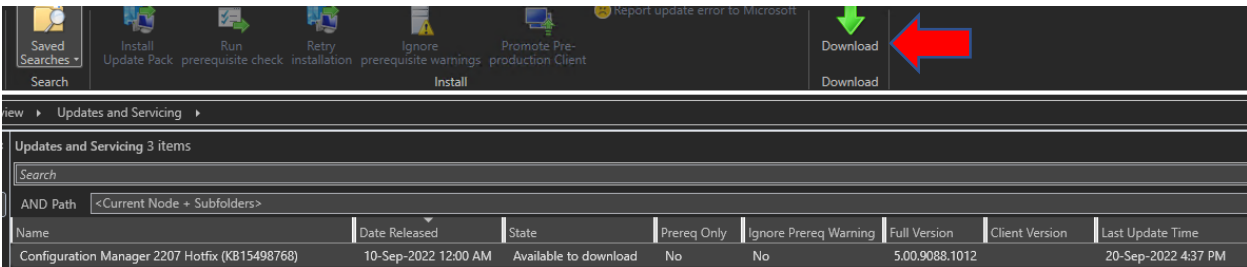
SQL

 Copy

```
select dbo.fnGetSecondarySiteCMUpdateStatus ('SiteCode_of_secondary_site')
```

If the value 1 is returned, the site is up to date, with all the hotfixes applied on its parent primary site.

If the value 0 is returned, the site has not installed all the fixes that are applied to the primary site, and you should use the **Recover Secondary Site** option to update the secondary site.



The screenshot shows the Configuration Manager console interface. At the top, there is a toolbar with various actions: Saved Searches, Install Update Pack, Run prerequisite check, Retry installation, Ignore prerequisite warnings, Promote Pre-production Client, and Report update error to Microsoft. The 'Download' button is highlighted with a red arrow. Below the toolbar, the breadcrumb navigation shows 'view > Updates and Servicing >'. The main content area displays 'Updates and Servicing 3 items' with a search bar and an AND Path dropdown set to '<Current Node + Subfolders>'. A table lists the updates:

Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version	Last Update Time
Configuration Manager 2207 Hotfix (KB15498768)	10-Sep-2022 12:00 AM	Available to download	No	No	5.00.9088.1012		20-Sep-2022 4:37 PM

Configuration Manager



Checking for updates. You can click Refresh to update the console to display recently downloaded updates. You can view information about the sync process in the Updates and Servicing Status node in the Monitoring workspace, or view the Dmpdownloader.log

OK

Saved Searches
 Install Update Pack
 Run prerequisite check
 Retry installation
 Ignore prerequisite warnings
 Promote Pre-production Client
 Report update error to Microsoft
 Download

ew > Updates and Servicing >

Updates and Servicing 3 items

Search

AND Path <Current Node + Subfolders>

Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version	Last Update Time
Configuration Manager 2207 Hotfix (KB15498768)	10-Sep-2022 12:00 AM	Ready to install	No	No	5.00.9088.1012		20-Sep-2022 4:59 PM

Configuration Manager Updates Wizard

General

Configuration Manager 2207 Hotfix (KB15498768)

This wizard helps you configure and install this update. [Learn more about updates for Configuration Manager.](#)

This version includes:

Configuration Manager site server updates

Prerequisite warnings:

Ignore any prerequisite check warnings and install this update regardless of missing requirements.

[Privacy Statement](#)

< Previous **Next >** Summary Cancel

Configuration Manager Updates Wizard

License Terms

Review and accept the terms for this update pack

You must accept the License Terms and Privacy Statement to continue installation.

[View the Microsoft Endpoint Configuration Manager License Terms](#)
[View the Microsoft Connected Cache License Terms](#)
[View the Microsoft Edge WebView2 Runtime License Terms](#)
[View the Privacy Statement](#)

I accept these License Terms and Privacy Statement.

[Learn more about licensing and Software Assurance](#)

< Previous **Next >** Summary Cancel



Summary



- General
- License Terms
- Summary**
- Progress
- Completion

Confirm the settings

Details:

Summary of update package installation
Install Update Package Configuration Manager 2207 Hotfix (KB15498768)
Prerequisite warnings will be ignored

To change these settings, click Previous. To apply the settings, click Next.


- < Previous
- Next >**
- Summary
- Cancel



Completion



- General
- License Terms
- Summary
- Progress
- Completion**

 **The task "Configuration Manager Updates Wizard" completed successfully**

Details:

Summary of update package installation
 **Success:** Install Update Package Configuration Manager 2207 Hotfix (KB15498768)
Prerequisite warnings will be ignored

To exit the wizard, click Close.

- < Previous
- Next >
- Summary
- Close**

Updates and Servicing 3 items

Search

AND Path <Current Node + Subfolders>

Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version	Last Update Time
Configuration Manager 2207 Hotfix (KB15498768)	10-Sep-2022 12:00 AM	Installing	No	Yes	5.00.9088.1012		20-Sep-2022 5:05 PM

Updates and Servicing 3 items

Search

AND Path <Current Node + Subfolders>

Name	Date Released	State	Prereq Only	Ignore Prereq Warning	Full Version	Client Version	Last Update Time
Configuration Manager 2207 Hotfix (KB15498768)	10-Sep-2022 12:00 AM	Installed	No	Yes	5.00.9088.1012		20-Sep-2022 5:13 PM

Update Pack Installation Status ✕

Detailed status for the Configuration Manager 2207 Hotfix (KB15498768) installation on the site TOR: Refresh

[View Post-Setup Configuration tasks](#)

Name	Status	Last Update Time
✓ Download	Completed	20-Sep-2022 4:59:10 PM
✓ Replication	Completed	20-Sep-2022 5:06:28 PM
⚠ Prerequisite Check	Completed with ...	20-Sep-2022 5:06:57 PM
✓ Installation	Completed	20-Sep-2022 5:13:40 PM
✓ Post Installation	Completed	20-Sep-2022 5:15:11 PM

Name	Status	Last Update Time	Description
✓ Installing SMS_EXECUTIVE service	Completed	20-Sep-2022 5:14:40 PM	Installing SMS_EXECUTIVE service
✓ Installing SMS_DATABASE_NOTIFICATION_MONITORING component	Completed	20-Sep-2022 5:14:40 PM	Installing SMS_DATABASE_NOTIFICATION_MONITORING component
✓ Installing SMS_HIERARCHY_MANAGER component	Completed	20-Sep-2022 5:14:40 PM	Installing SMS_HIERARCHY_MANAGER component
✓ Installing SMS_REPLICATION_CONFIGURATION_MONITORING component	Completed	20-Sep-2022 5:14:40 PM	Installing SMS_REPLICATION_CONFIGURATION_MONITORING component
✓ Monitoring replication initialization	Completed	20-Sep-2022 5:14:40 PM	Monitoring database replication
✓ Updating Configuration Manager Client Preproduction Package	Completed	20-Sep-2022 5:14:52 PM	Updating StagingClient folder
✓ Updating Client folder on Site Server	Completed	20-Sep-2022 5:15:11 PM	Updating Client folder
✓ Updating Configuration Manager Client Package	Completed	20-Sep-2022 5:15:11 PM	Updating Client folder

Description:

[Completed]:Installing SMS_EXECUTIVE service on Site Server. Check sitecomp.log for details.

OK Cancel

This concludes installing above KB.

Thanks

Ram
20th Sep 2022