

SlashNext Windows Microsoft Endpoint Configuration Manager (MECM) Guide

TABLE OF CONTENTS

1 INTRODUCTION	2
2 CREATE A NETWORK SHARED PATH	2
3 DEPLOY SLASHNEXT PHISHING PROTECTION INSTALLER PACKAGE	2
4 VERIFY INSTALLATION OF BROWSER EXTENSIONS ON USER'S MACHINE	15
5 SILENT INSTALLATION OF SLASHNEXT INSTALLER WITH INSTALL PARAMETERS	16
Switches and Parameters	17

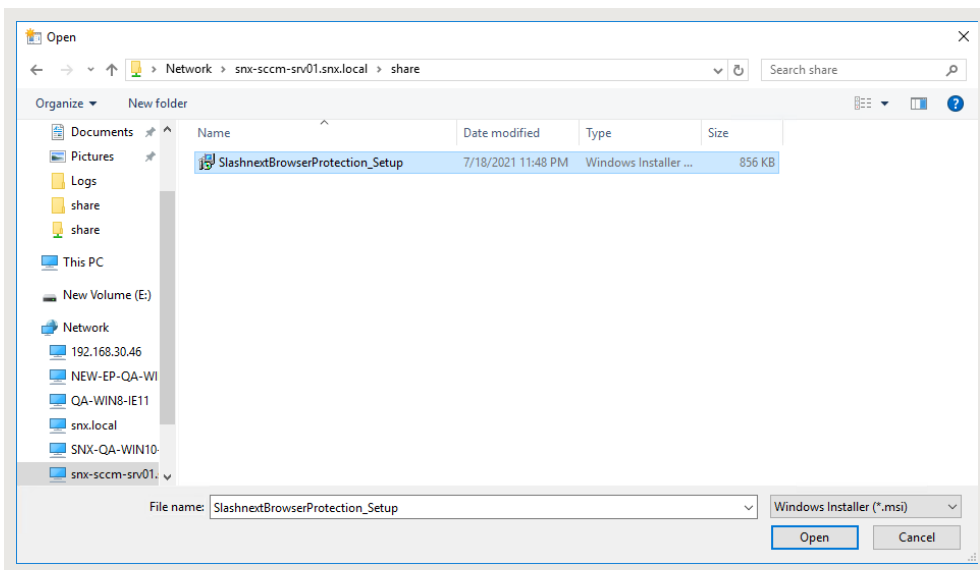
1 | INTRODUCTION

This document describes how SlashNext Browser Protection Installer will install and activate Chrome, Firefox, and Edge extensions on devices managed from Microsoft Endpoint Configuration Manager (MECM).


2 | CREATE A NETWORK SHARED PATH

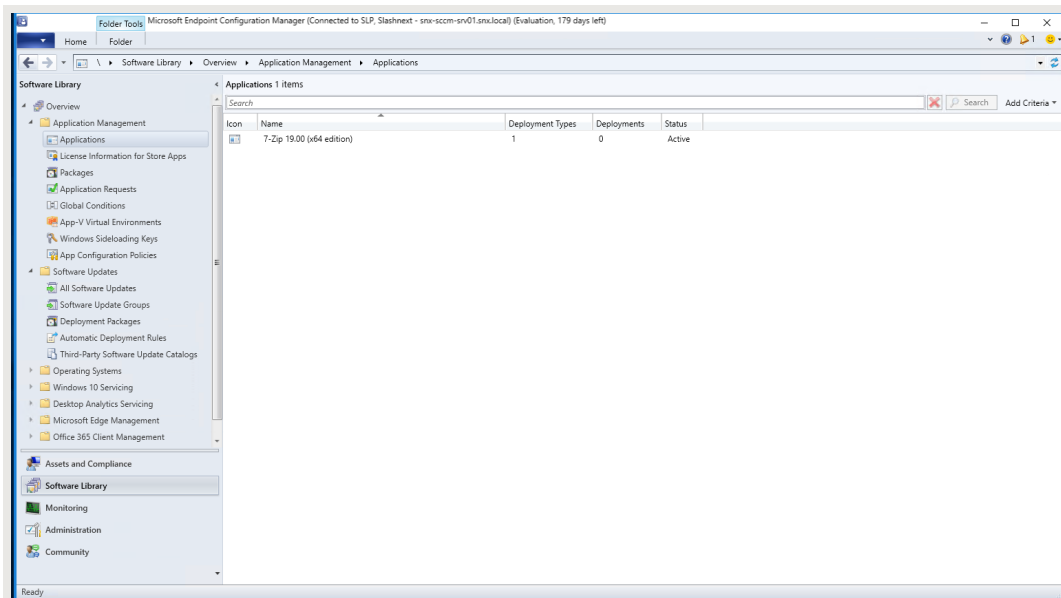
The first step in deploying SlashNext Phishing Protection installer through Microsoft Endpoint Configuration Manager is to create a network shared path on the publishing server. This can be done by following these steps:

1. Log on to the server as an Administrator user.
2. Create a shared network folder (this folder will contain our MSI package).
3. Copy the SlashNext Browser Protection MSI in the shared folder.

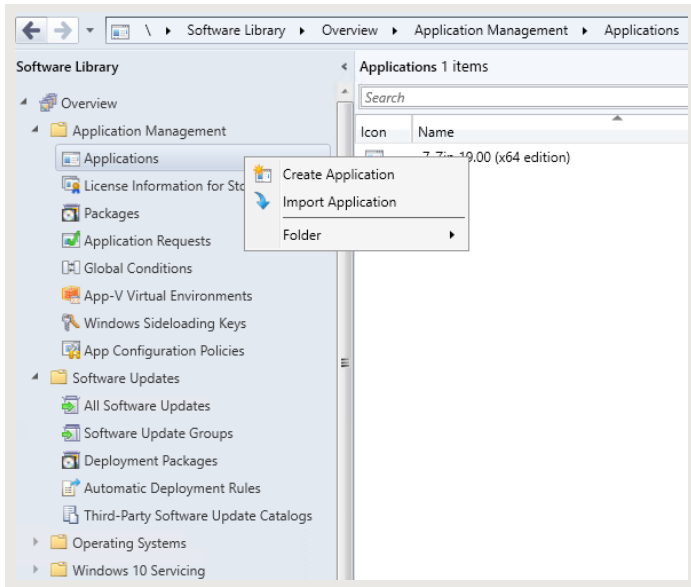


3 | DEPLOY SLASHNEXT PHISHING PROTECTION INSTALLER PACKAGE

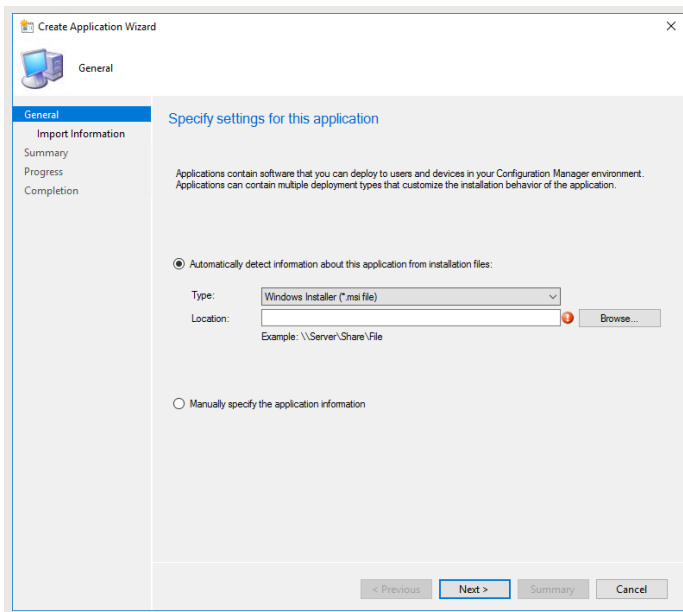
1. Open the Microsoft Configuration Manager Console. 
2. Go to: **Software Library\Application Management\Applications**.



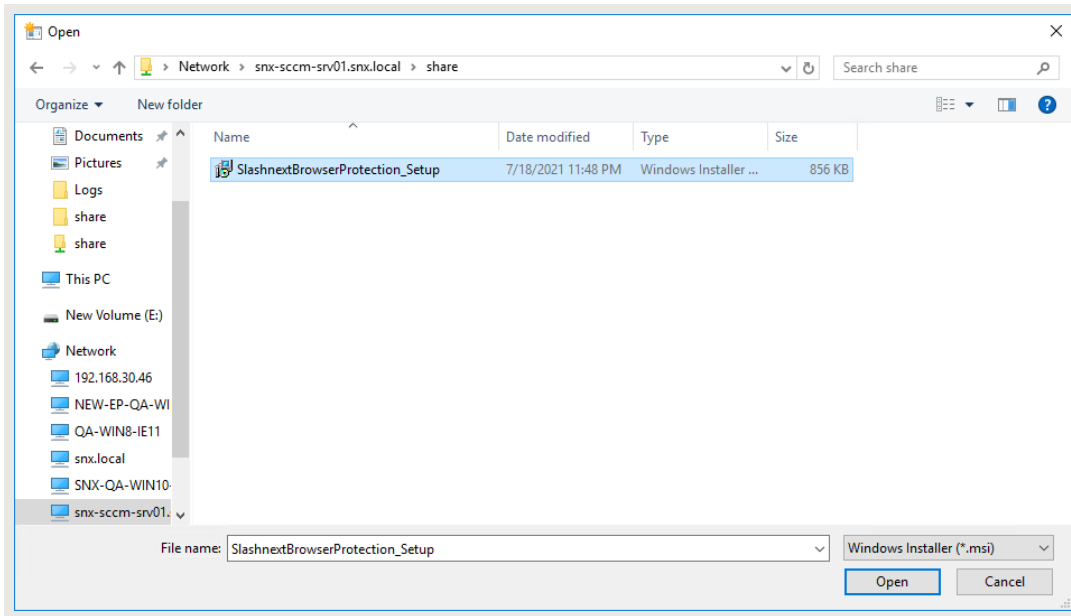
3. Right click on "Applications" and click on "Create Application" option.



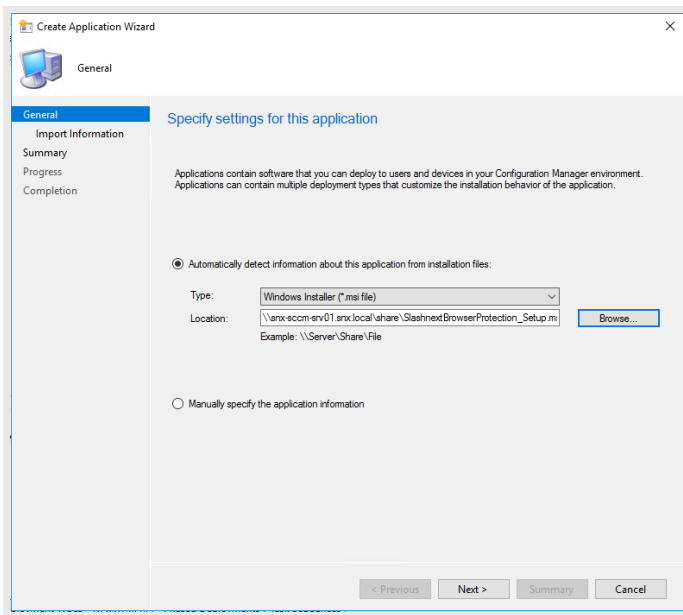
4. Select option "Automatically detect information about this application from installation files" as shown in window.
5. Select option Windows Installer (*.msi file) from Type drop down.



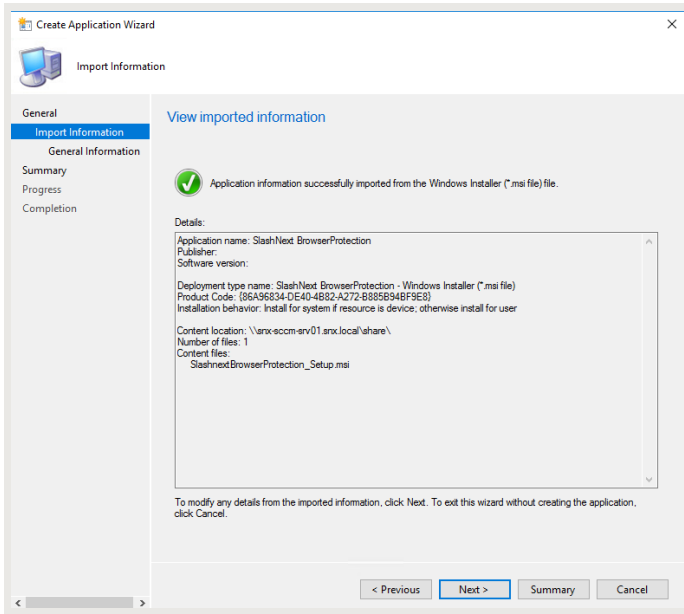
6. Click **Browse** and specify location of installer. e.g \\Server Name\share\SlashnextBrowserProtection_Setup.msi



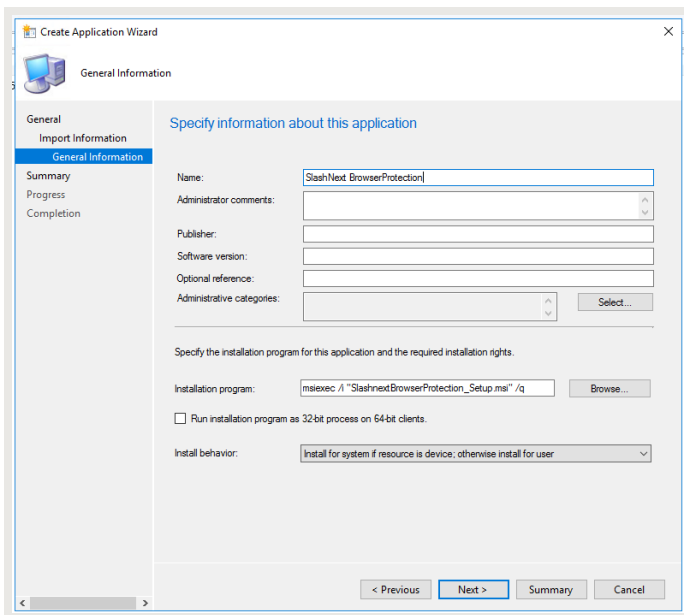
7. On selection of File **General** tab is filled with information.



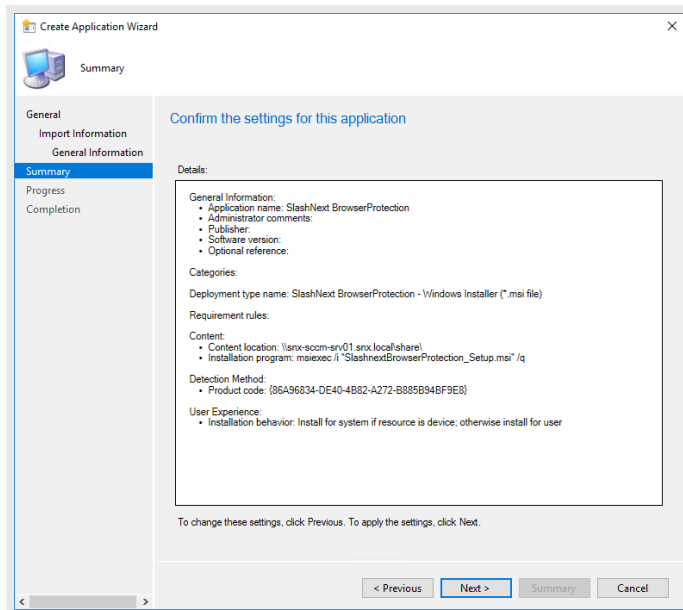
8. Click "Next".



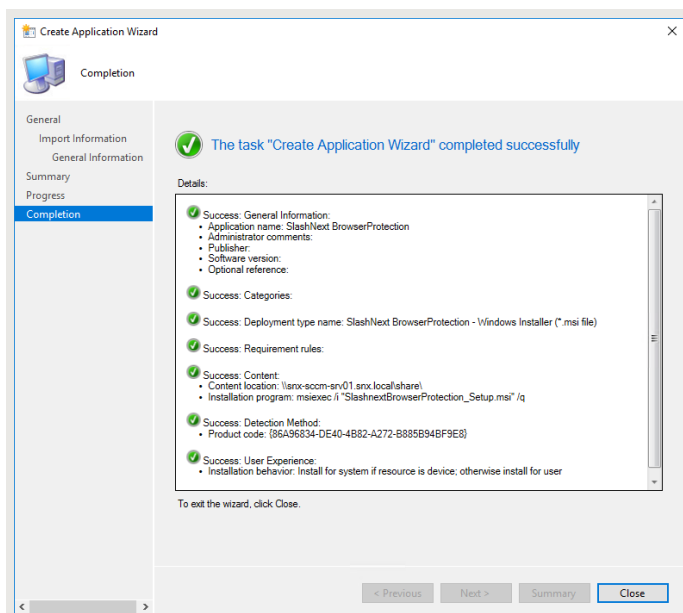
9. In **General Information** fill the fields according to your requirement and Click on **Next** button.



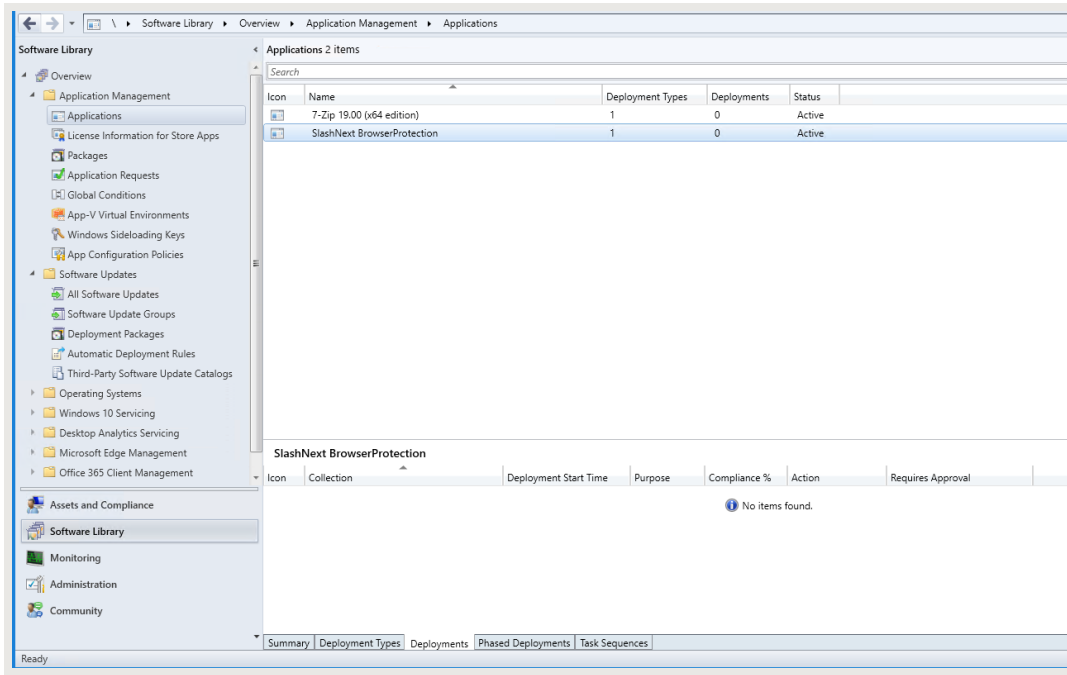
10. In **Summary** click on **Next** button.



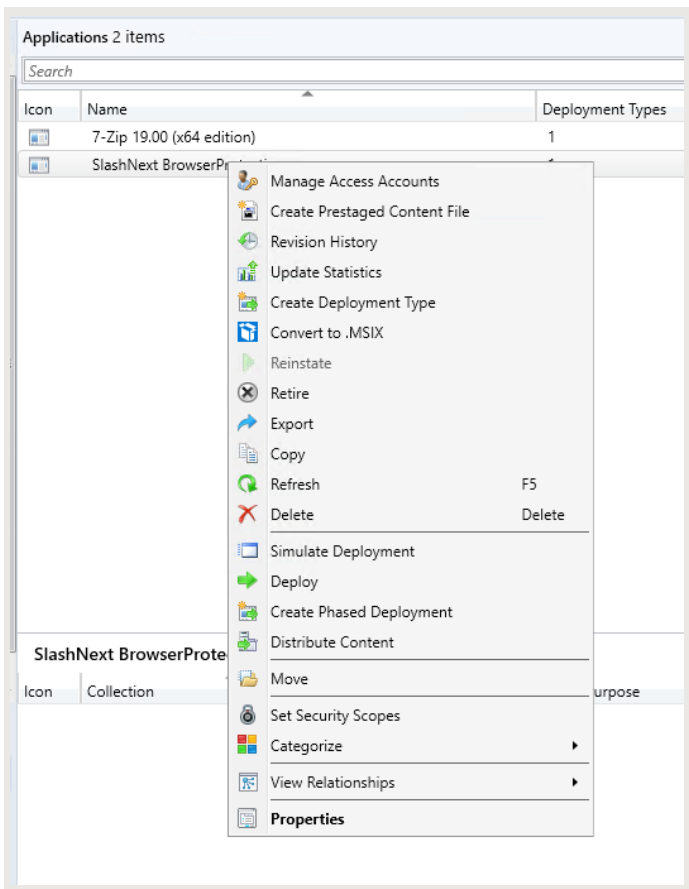
11. Once the application is created. Click on **Close** button.



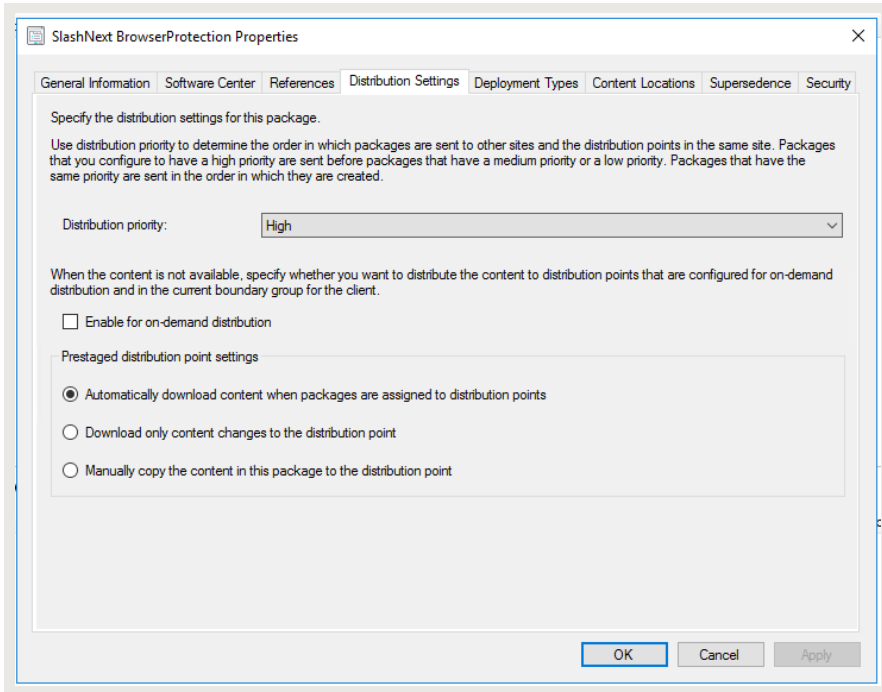
12. Now you can see SlashNext Browser Protection MSI in your Applications.



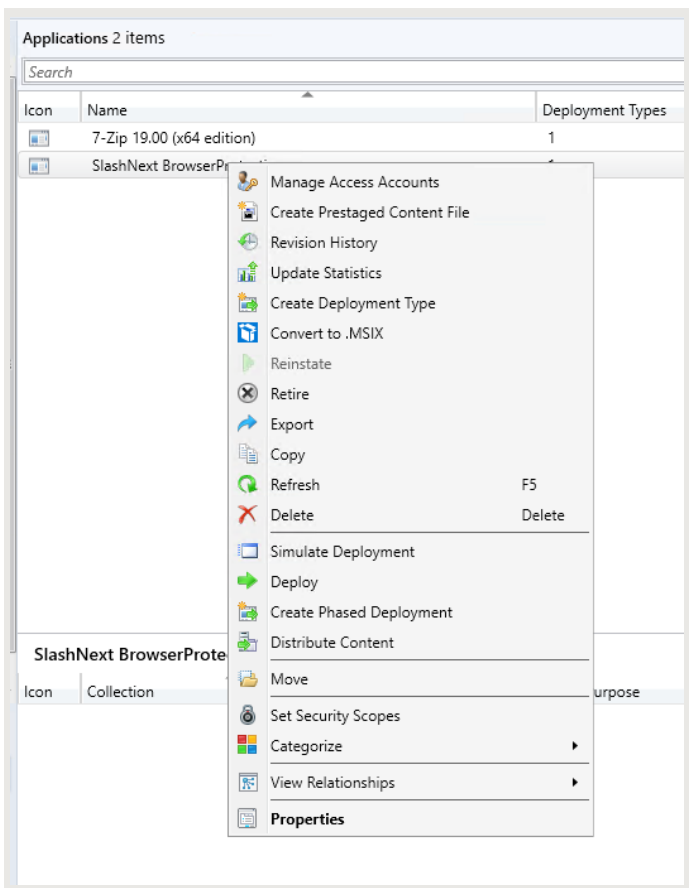
13. Right Click on SlashNext Browser Protection MSI and click on **Properties**.



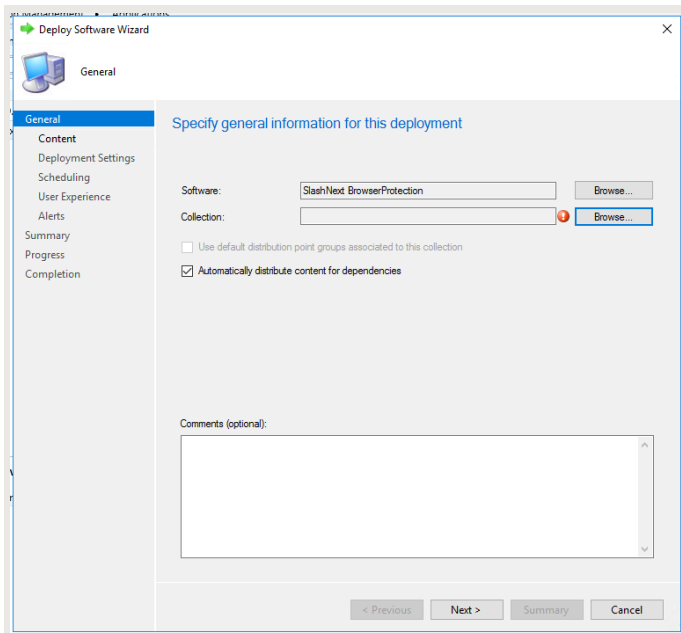
14. Click on **Distribution Settings**. In *Distribution Priority* select value to **High**.
15. In **Prestaged distribution point settings** select "*Automatically download content when packages are assigned to distribution points*".
16. Click **OK** button to proceed.



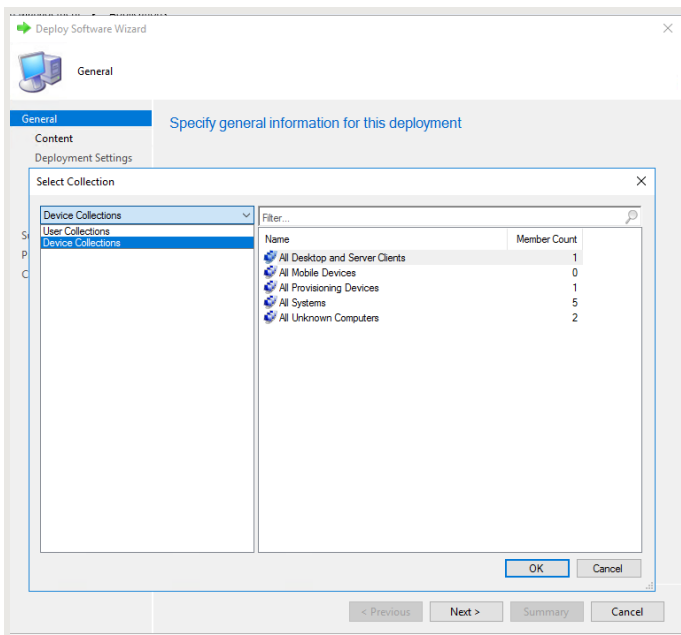
17. Right Click on SlashNext Browser Protection MSI and click on **Deploy** to deploy application.



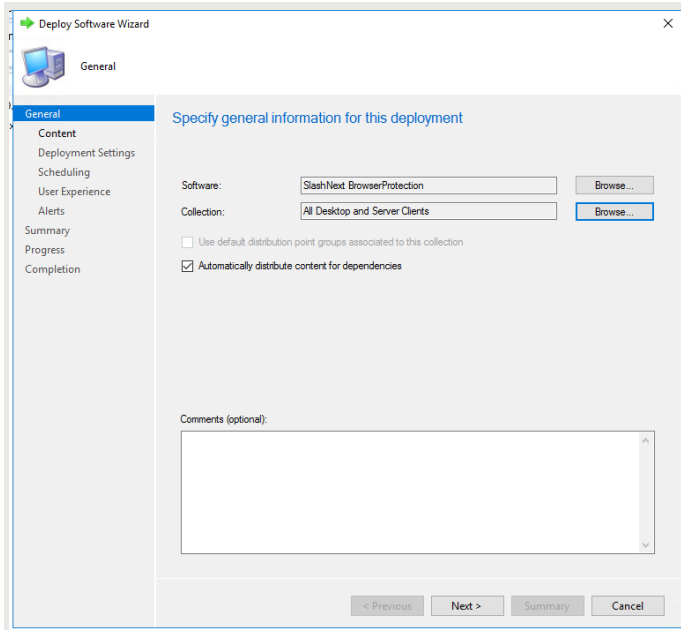
18. Deploy Software Wizard will open.



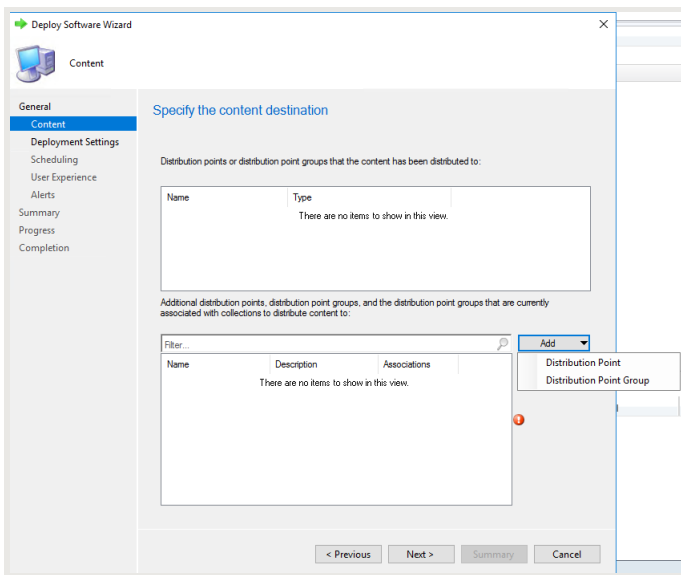
19. Click on **Browse** to select Collection. Select User or Device Collection according to your requirement. Click on **OK**.



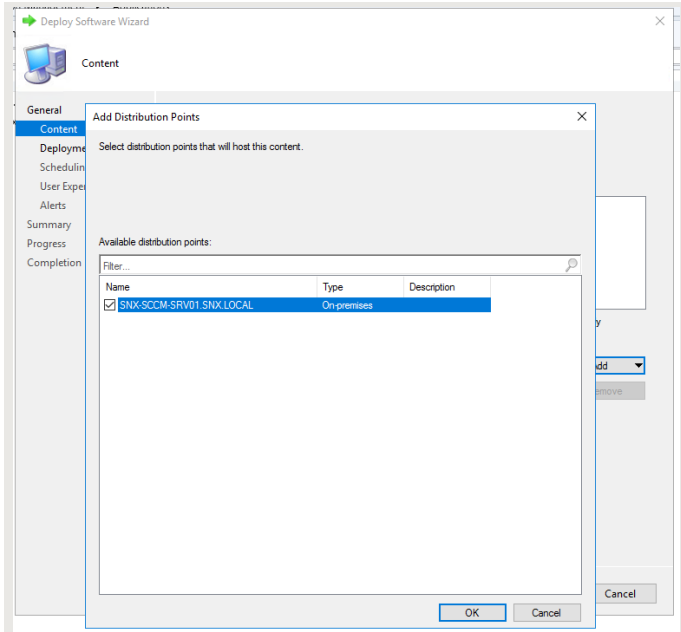
20. Select "Automatically distribute content for dependencies". Click on Next button.



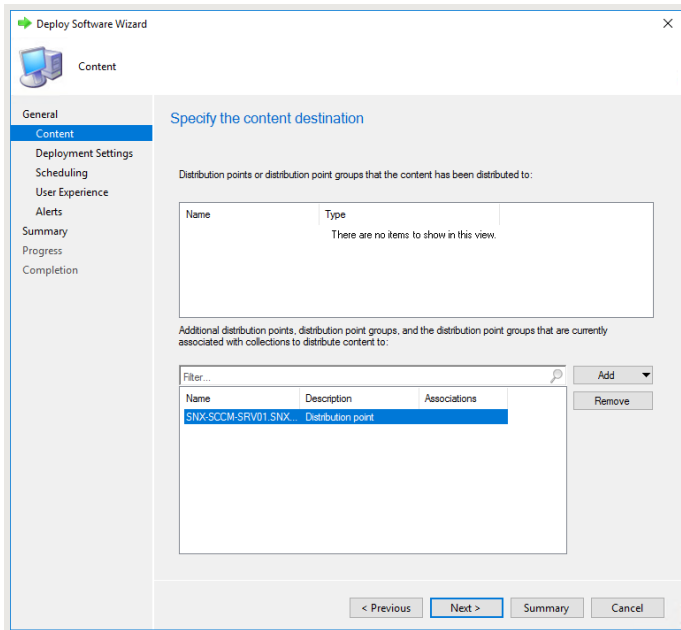
21. Click on Add button to select Distribution Point.



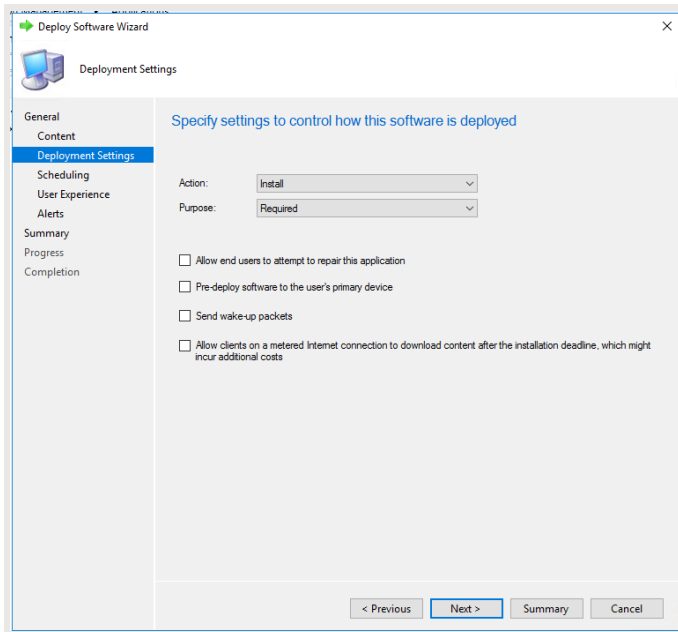
22. Select distribution points that will host this content and Click on **OK** button.



23. Distribution point will be added in your content destination. Click on **Next** button.



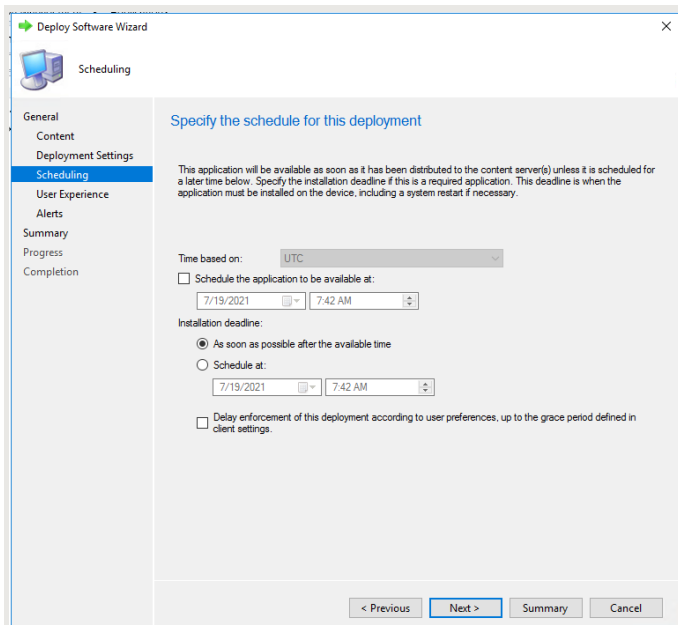
24. In Deployment Settings select *Action* as **Install** and *Purpose* as **Required**.
25. Click on **Next** button to continue.



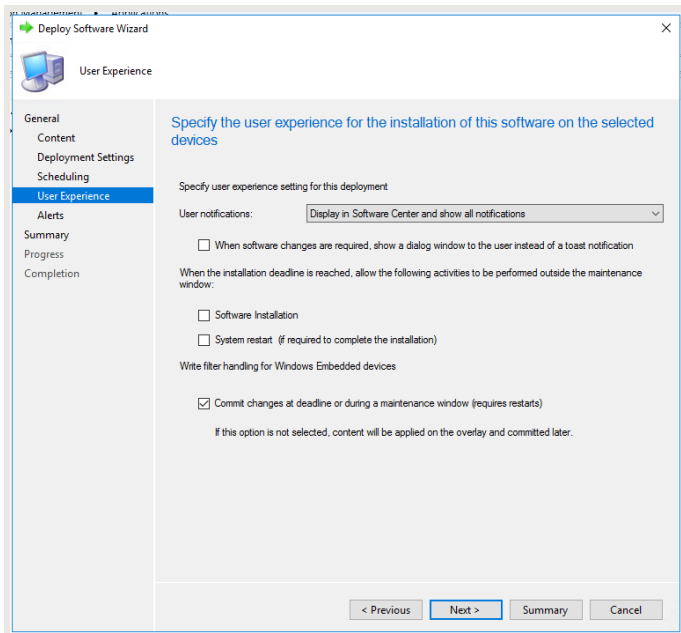
26. Schedule deployment according to your own requirement. Click **Next** on Scheduling screen.

Note

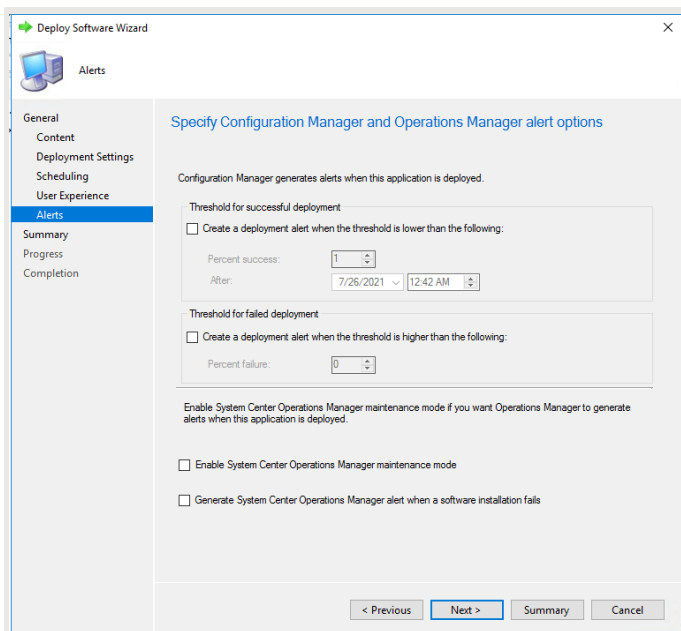
Select "*As soon as possible after the available time*" in **Installation deadline** for quick installation.



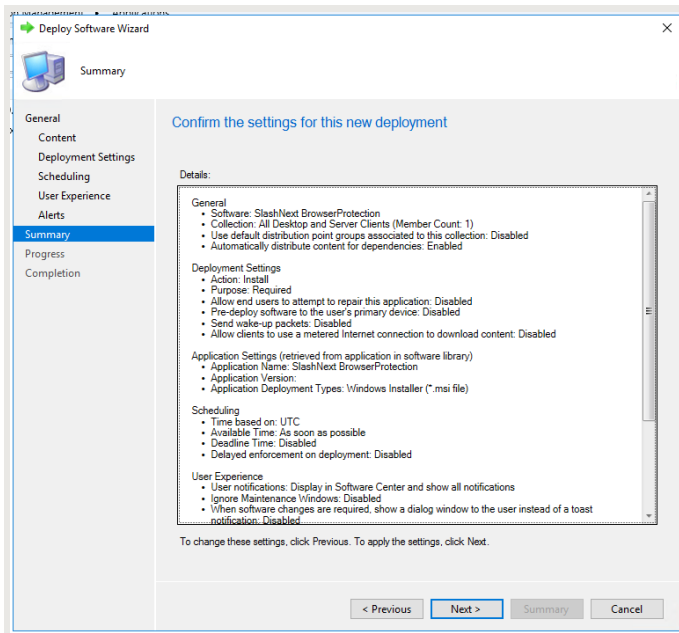
27. Select **User Experience** according to your requirement and click **Next** to continue.



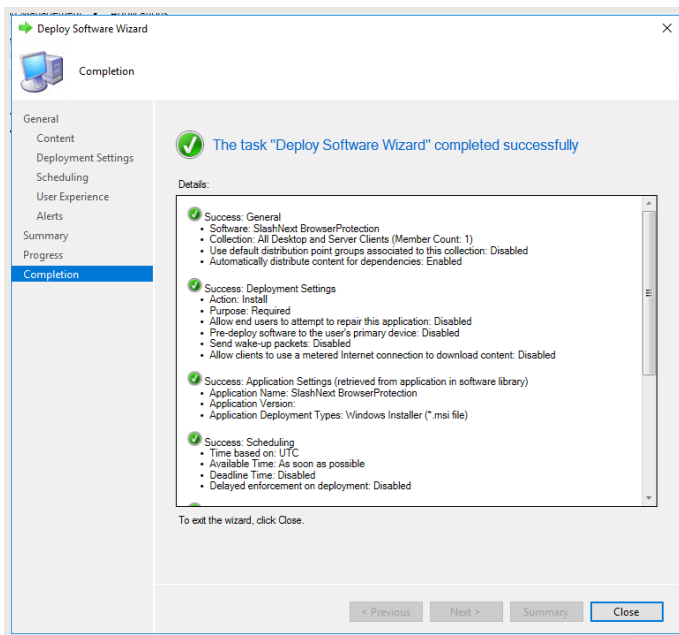
28. Select **Alerts** according to your requirement and click **Next** to continue.



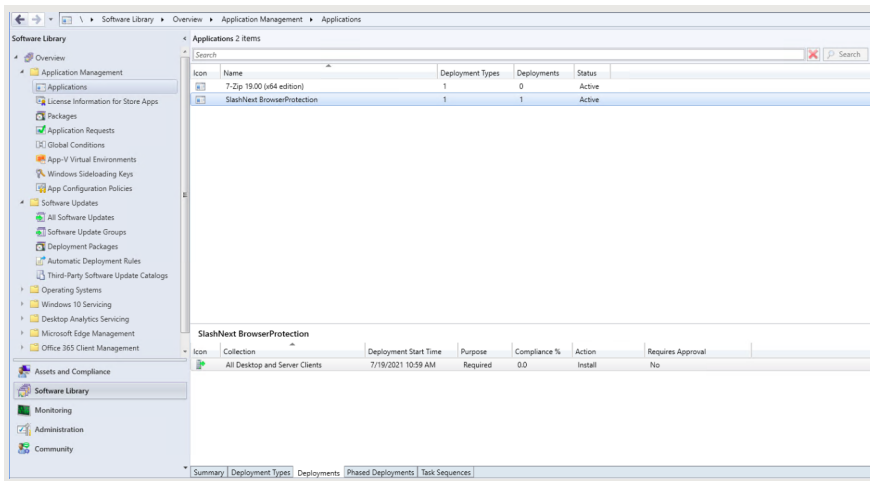
29. Click **Next** on Summary screen.



30. Click on **Close** button for deployment completion.



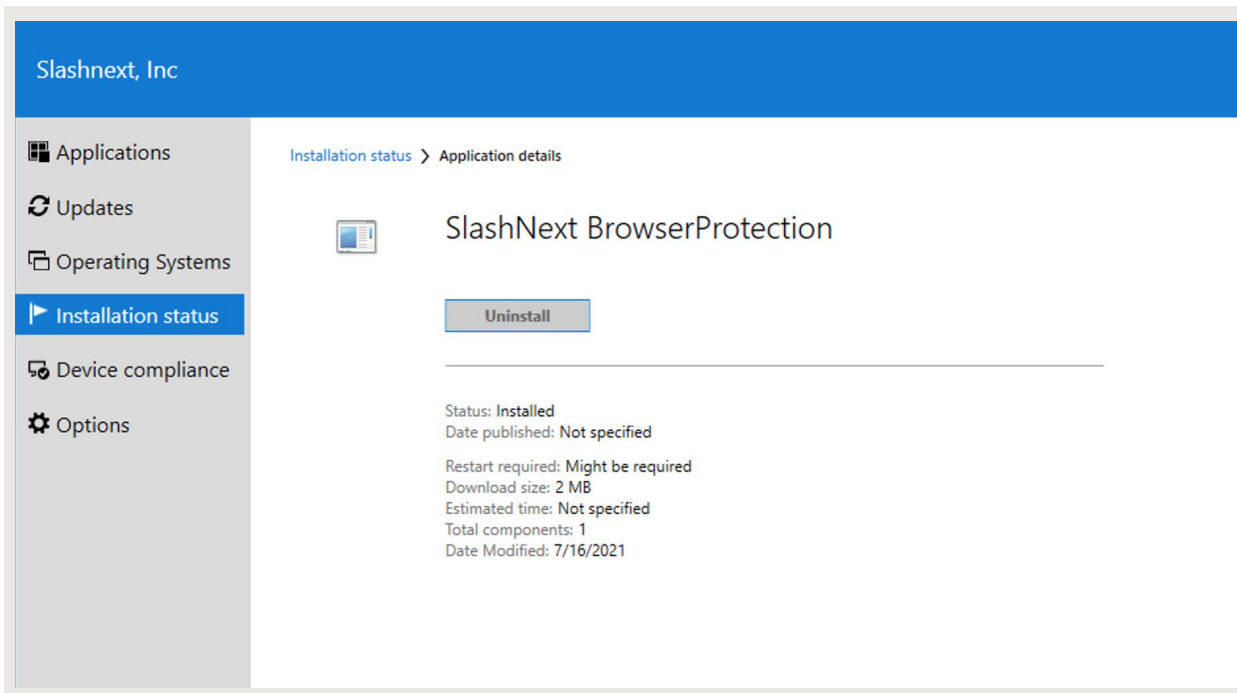
31. After successful addition, Installer name is shown in **Applications List**.



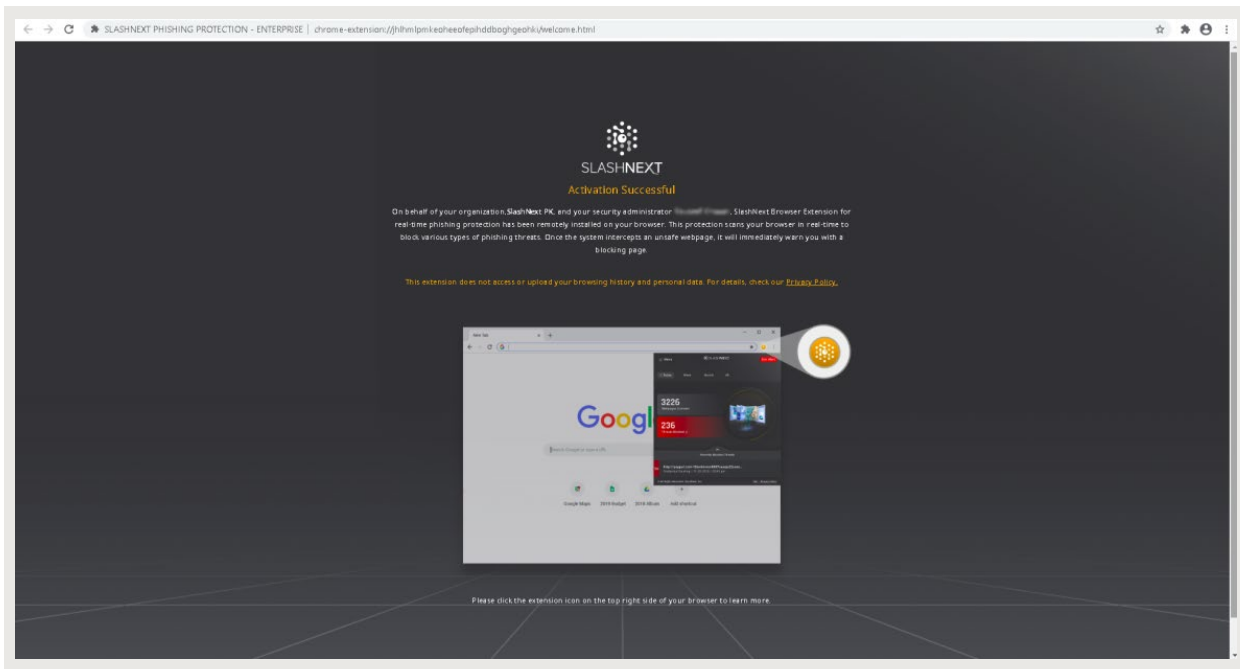
4 | VERIFY INSTALLATION OF BROWSER EXTENSIONS ON USER'S MACHINE

Follow these steps to verify the installation of Browser Extensions.

1. Sign in to Microsoft Endpoint Configuration Manager domain managed client.
2. Open **Software Center** on Client machine and Click on **Installation Status** to check installation status.

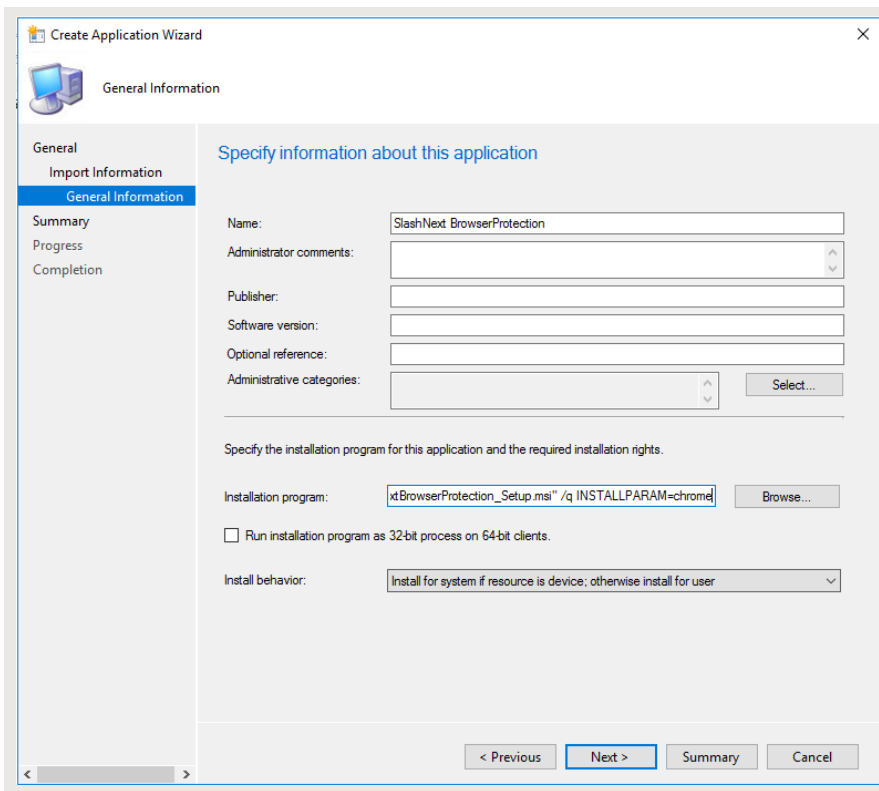


3: Open Chrome, Firefox, or Edge Chromium browser. SlashNext Browser Protection extension icon will appear on the right corner of the address bar and the extension Activation Successful page will appear in the browser tab.



5 | SILENT INSTALLATION OF SLASHNEXT INSTALLER WITH INSTALL PARAMETERS

Optionally, you can enter Additional command line options that you want to apply to the MSI file when it runs. To add command line parameter in MECM, Add command line argument in **Step 9**.



5.1 | SWITCHES AND PARAMETERS

The following table lists all the switches and possible enrollment parameters you can enter into command line and respective description and values for each parameter.

INSTALLPARAM=Value	<p>Enter value chrome for installation of Chrome extension</p> <p>Enter value firefox for installation of Firefox extension</p> <p>Enter value edge for installation of Edge Chromium extension</p> <p>Enter value chrome,firefox for installation of Chrome and Firefox extensions</p> <p>Enter value chrome,edge for installation of Chrome and Edge Chromium extensions</p> <p>Enter value firefox,edge for installation of Firefox and Edge Chromium extensions</p> <p>Enter value chrome,firefox,edge for installation of Chrome,Firefox and Edge Chromium extensions</p>
--------------------	---

The following syntax is used in MECM command line where value is added to install extension on specified browser.

INSTALLPARAM=value

To install Chrome extension, the following syntax is used:

INSTALLPARAM=chrome

To install extension to more than 1 supported browser, a comma separated value is used. To install Chrome and Firefox extensions, the following syntax is used.

INSTALLPARAM=chrome,firefox

INSTALLPARAM value can be <chrome/firefox/edge/chrome,firefox/chrome,edge/firefox,edge/chrome,firefox,edge> according to requirement. Initiating any one of these examples silently installs the product without prompting the user to select any of the acknowledgment buttons.

Note

If INSTALLPARAM is not given all Chrome, Firefox and Edge Chromium extensions will get installed silently.