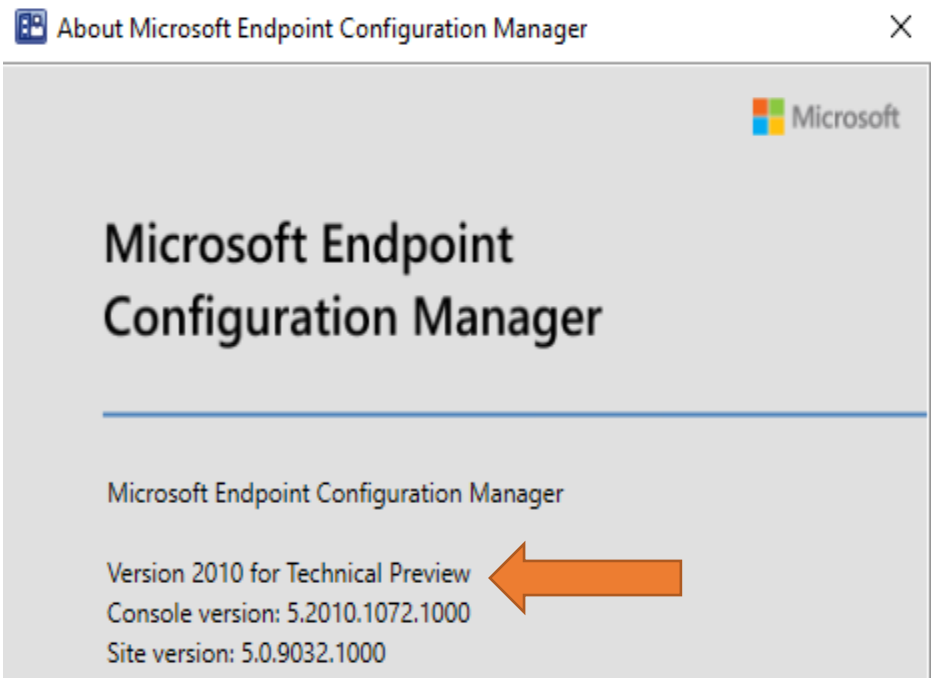
Installing Technical Preview 2010.2

In this post, I will show you how to install TP2010.2 and explore new features. I am currently running TP2010. Will upgrade to TP2010.2 from the console.

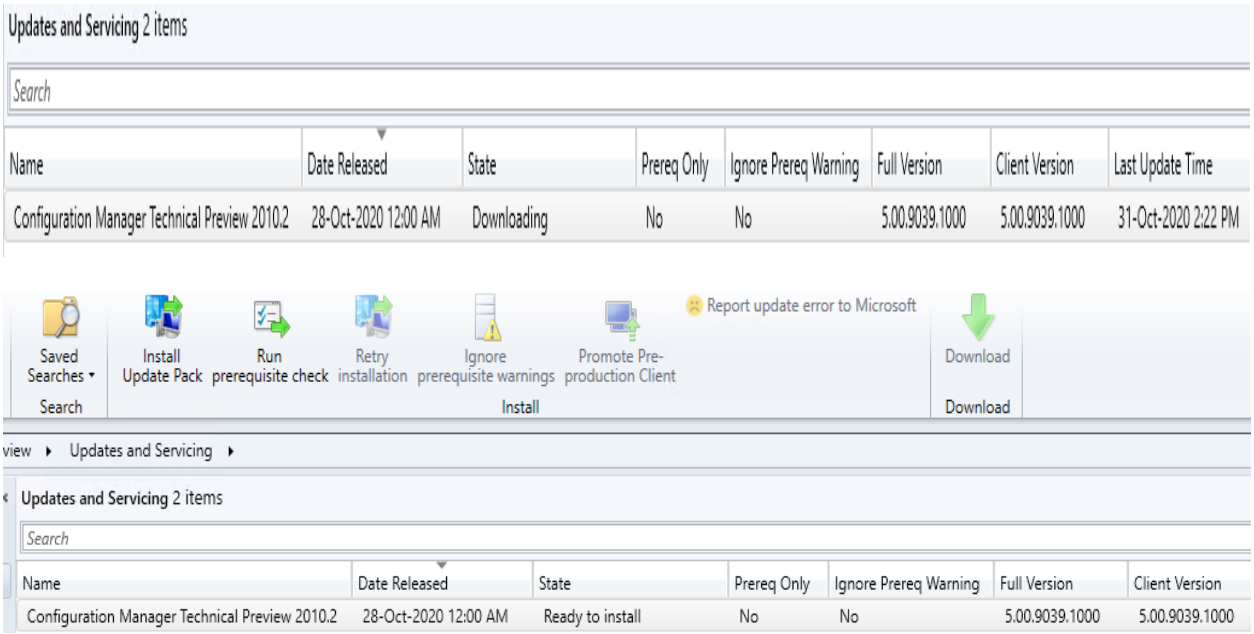


Below are the links to TP2010.2 documentation.

https://docs.microsoft.com/en-us/mem/configmgr/core/get-started/2020/technical-preview-2010-2

https://techcommunity.microsoft.com/t5/configuration-manager-blog/new-application-actions-in-mem-admin-center-with-configuration/ba-p/1838207

Just clicked check for updates and it is downloading TP2010.2



Configuration Manager Updates Wizard

General

- General
  - Features
  - Client Update Options
- License Terms
- Summary
- Progress
- Completion

Configuration Manager Technical Preview 2010.2

This wizard helps you configure and install this update.

Learn more.

This version includes:

Configuration Manager site server updates
Configuration Manager console updates
Configuration Manager client updates
Fixes for known issues
New features

Prerequisite warnings:

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

Privacy Statem

< Previous | Next > | Summary | Cancel

Configuration Manager Updates Wizard

Client Update Options

- General
  - Features
  - Client Update Options
- License Terms
- Summary
- Progress
- Completion

Client Update Settings

This update includes an update for the Configuration Manager client. You can upgrade your clients immediately, or validate this client in a pre-production collection before you upgrade all your Configuration Manager clients.

◉ Upgrade without validating

Overwrites your current Configuration Manager client package with the new client update. All new client installations and client upgrades use this new client update.

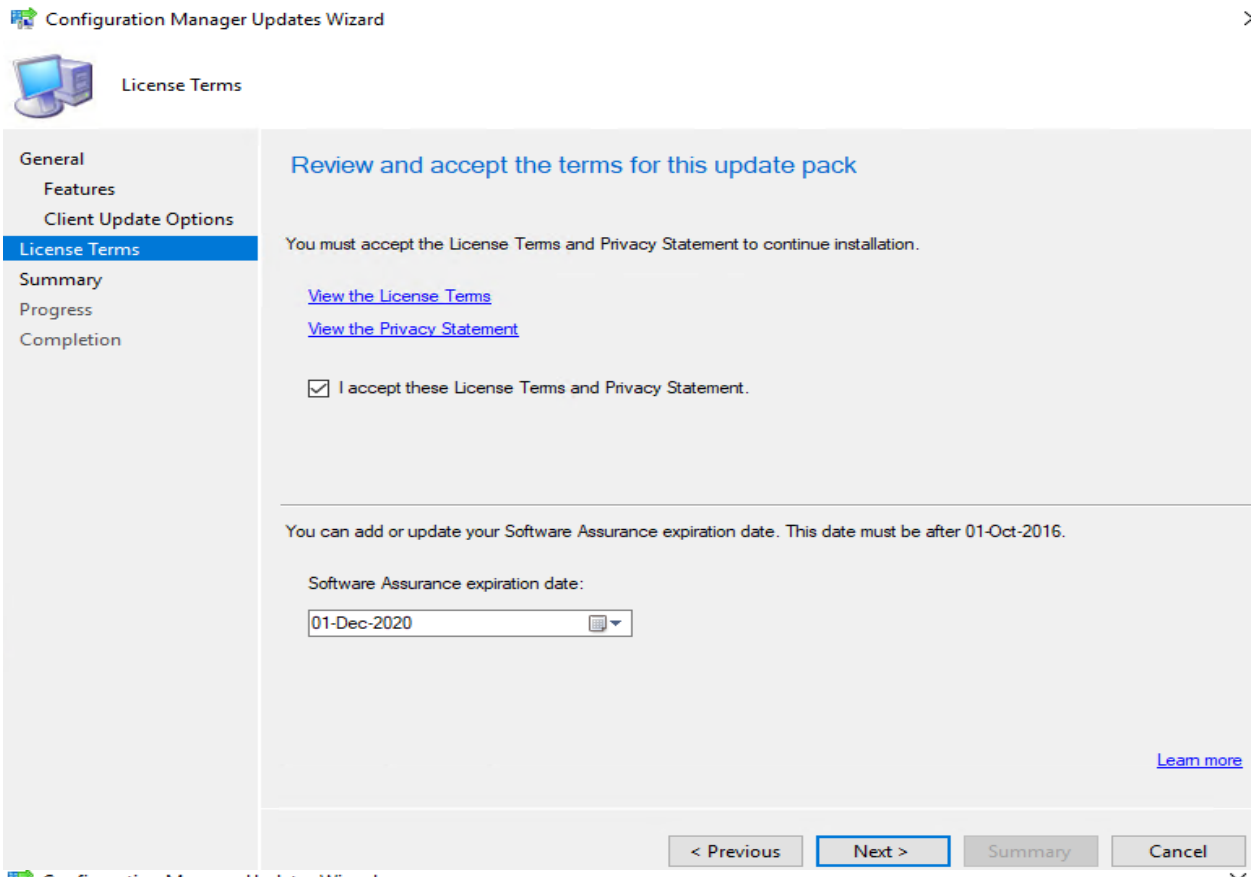
○ Validate in pre-production collection

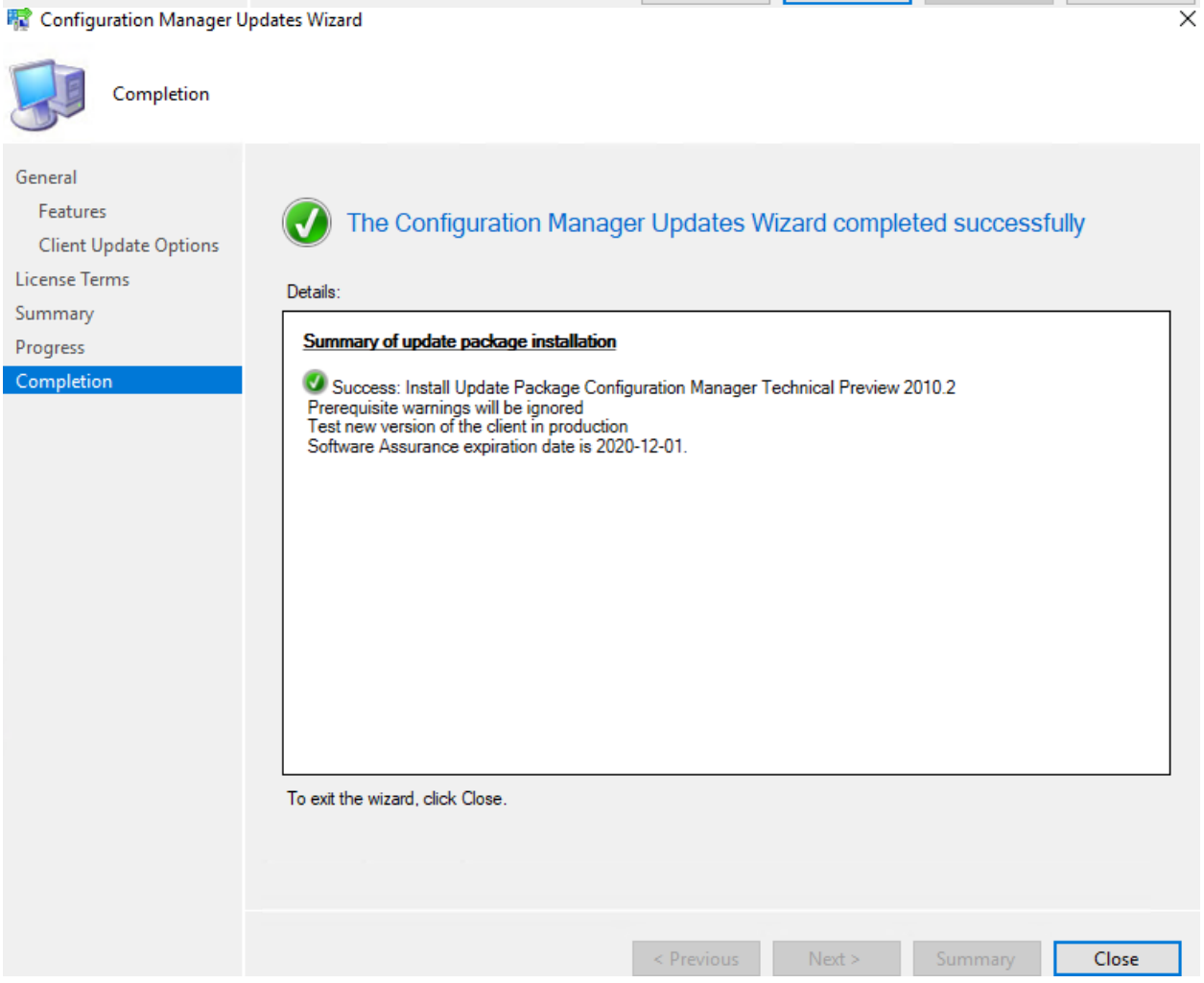
Validate the client update on members of the pre-production collection while you keep your production client package intact. Later, you can overwrite the production package using Client Update Options in the Updates and Servicing node of the Configuration Manager console.

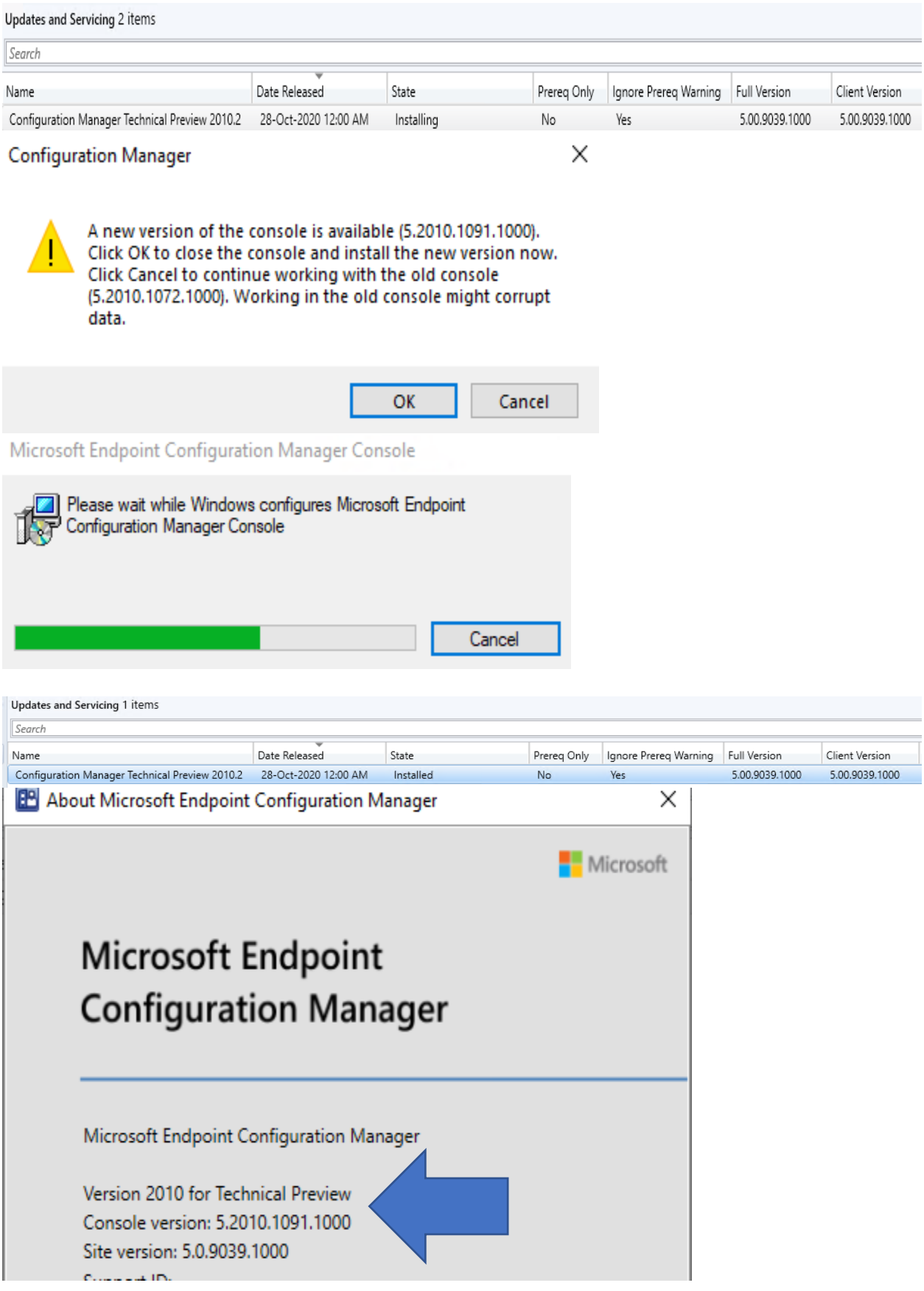
Pre-production collection:

Browse...

< Previous | Next > | Summary | Cancel


Configuration Manager Updates Wizard
License Terms
General
Features
Client Update Options
License Terms
Summary
Progress
Completion
Review and accept the terms for this update pack
You must accept the License Terms and Privacy Statement to continue installation.
View the License Terms
View the Privacy Statement
I accept these License Terms and Privacy Statement.
You can add or update your Software Assurance expiration date. This date must be after 01-Oct-2016.
Software Assurance expiration date:
01-Dec-2020
Learn more
< Previous
Next >
Summary
Cancel


Configuration Manager Updates Wizard
Completion
General
Features
Client Update Options
License Terms
Summary
Progress
Completion
The Configuration Manager Updates Wizard completed successfully
Details:
Summary of update package installation
Success: Install Update Package Configuration Manager Technical Preview 2010.2
Prerequisite warnings will be ignored
Test new version of the client in production
Software Assurance expiration date is 2020-12-01.
To exit the wizard, click Close.
< Previous
Next >
Summary
Close


Updates and Servicing 2 items
Search
Name
Date Released
State
Prereq Only
Ignore Prereq Warning
Full Version
Client Version
Configuration Manager Technical Preview 2010.2
28-Oct-2020 12:00 AM
Installing
No
Yes
5.00.9039.1000
5.00.9039.1000
Configuration Manager
A new version of the console is available (5.2010.1091.1000). Click OK to close the console and install the new version now. Click Cancel to continue working with the old console (5.2010.1072.1000). Working in the old console might corrupt data.
OK
Cancel
Microsoft Endpoint Configuration Manager Console
Please wait while Windows configures Microsoft Endpoint Configuration Manager Console
Cancel
Updates and Servicing 1 items
Search
Name
Date Released
State
Prereq Only
Ignore Prereq Warning
Full Version
Client Version
Configuration Manager Technical Preview 2010.2
28-Oct-2020 12:00 AM
Installed
No
Yes
5.00.9039.1000
5.00.9039.1000
About Microsoft Endpoint Configuration Manager
Microsoft
Microsoft Endpoint Configuration Manager
Microsoft Endpoint Configuration Manager
Version 2010 for Technical Preview
Console version: 5.2010.1091.1000
Site version: 5.0.9039.1000

NEW FEATURES:

All the new features are within Microsoft Endpoint Admin Center. I will provide just the screen shot from Microsoft document. I have not configured Intune or Cloud Management or E3/E5 license.

Tenant attach: Troubleshooting portal lists a user's devices based on usage

The troubleshooting portal in Microsoft Endpoint Manager admin center allows you to search for a user and view their associated devices. Starting in this release, tenant attached devices that are assigned user device affinity automatically based on usage will now be returned when searching for a user.

Prerequisites

- An environment that's tenant attached with uploaded devices
- Install the latest version of the Configuration Manager client.
- Target clients with **User and Device Affinity** client settings to automatically create the affinities.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

View a user's devices

1. Go to the Microsoft Endpoint Manager admin center.
2. Select **Troubleshooting + support**.
3. On the **Troubleshoot** page, select **Change user** then search for a user.
4. The **Devices** chart lists the ConfigMgr devices associated with the user.

    - Devices that previously reported affinity will resend their affinity to reflect in the admin center.
    - Devices that aren't already associated with a user will be updated once the affinity threshold has been met and reported.

Known issues

In this technical preview, these actions only work if the client used a self-signed certificate during registration. If the client registered using a PKI certificate or via Cloud Management Gateway, these actions won't work.

You can verify which clients will work by querying the Configuration Manager database. If **ApprovalStatus** is 1, the actions can be run. If the **ApprovalStatus** is 2 or 3, then the actions won't work.

SQL Copy

```
select s.Name0 as MachineName, c.ApprovalStatus from ClientKeyData c join system_disc s on c.smsid = s.SMS_Unique_Identi
```

select s.Name0 as MachineName, c.ApprovalStatus from ClientKeyData c join system_disc s on c.smsid = s.SMS_Unique_Identifier0

Improvements to deploy an OS over CMG using boot media

Technical preview branch version 2009 included support for using boot media to reimage internet-based devices that connect through a cloud management gateway (CMG).

This release streamlines the administrative workflow in the Configuration Manager console. On the **Media Management** page of the **Create Task Sequence Media Wizard**, the **Internet-based media** option no longer exists. Select the **Site-based media** option. Then still select the CMG for the management point on the **Boot Image** page.

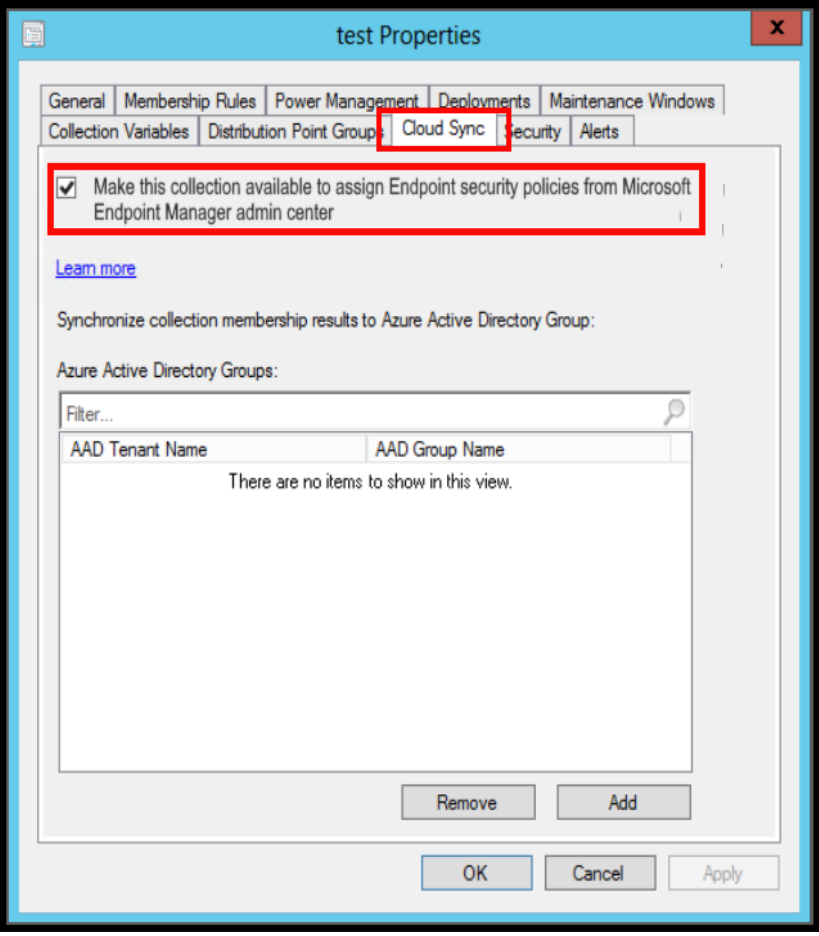
Make Configuration Manager collections available to assign Endpoint security policies

If you haven't already done so, make Configuration Manager collections available to assign Endpoint security policies.

1. From a Configuration Manager console connected to your top-level site, right-click on a device collection that you synchronize to Microsoft Endpoint Manager admin center and select **Properties**.

2. On the **Cloud Sync** tab, enable the option to **Make this collection available to assign Endpoint security policies from Microsoft Endpoint Manager admin center**.

    - You can't select this option if your Configuration Manager hierarchy isn't tenant attached.
    - The collections available for this option are limited by the collection scope selected for tenant attach upload.



Disable Azure AD authentication for onboarded tenants

You can now disable Azure Active Directory (Azure AD) authentication for tenants not associated with users and devices. When you onboard Configuration Manager to Azure AD, it allows the site and clients to use modern authentication. Currently, Azure AD device authentication is enabled for all onboarded tenants, whether or not it has devices. For example, you have a separate tenant with a subscription that you use for compute resources to support a cloud management gateway. If there aren't users or devices associated with the tenant, disable Azure AD authentication.

Try it out!

Try to complete the tasks. Then send Feedback with your thoughts on the feature.

1. In the Configuration Manager console, go to the **Administration** workspace.

2. Expand **Cloud Services** and select the **Azure Services** node.

3. Select the target connection of type **Cloud Management**. In the ribbon, select **Properties**.

4. Switch to the **Applications** tab.

5. Select the option to **Disable Azure Active Directory authentication for this tenant**.

6. Select **OK** to save and close the connection properties.

Configure and assign firewall policies

1. Go to the Microsoft Endpoint Manager admin center.

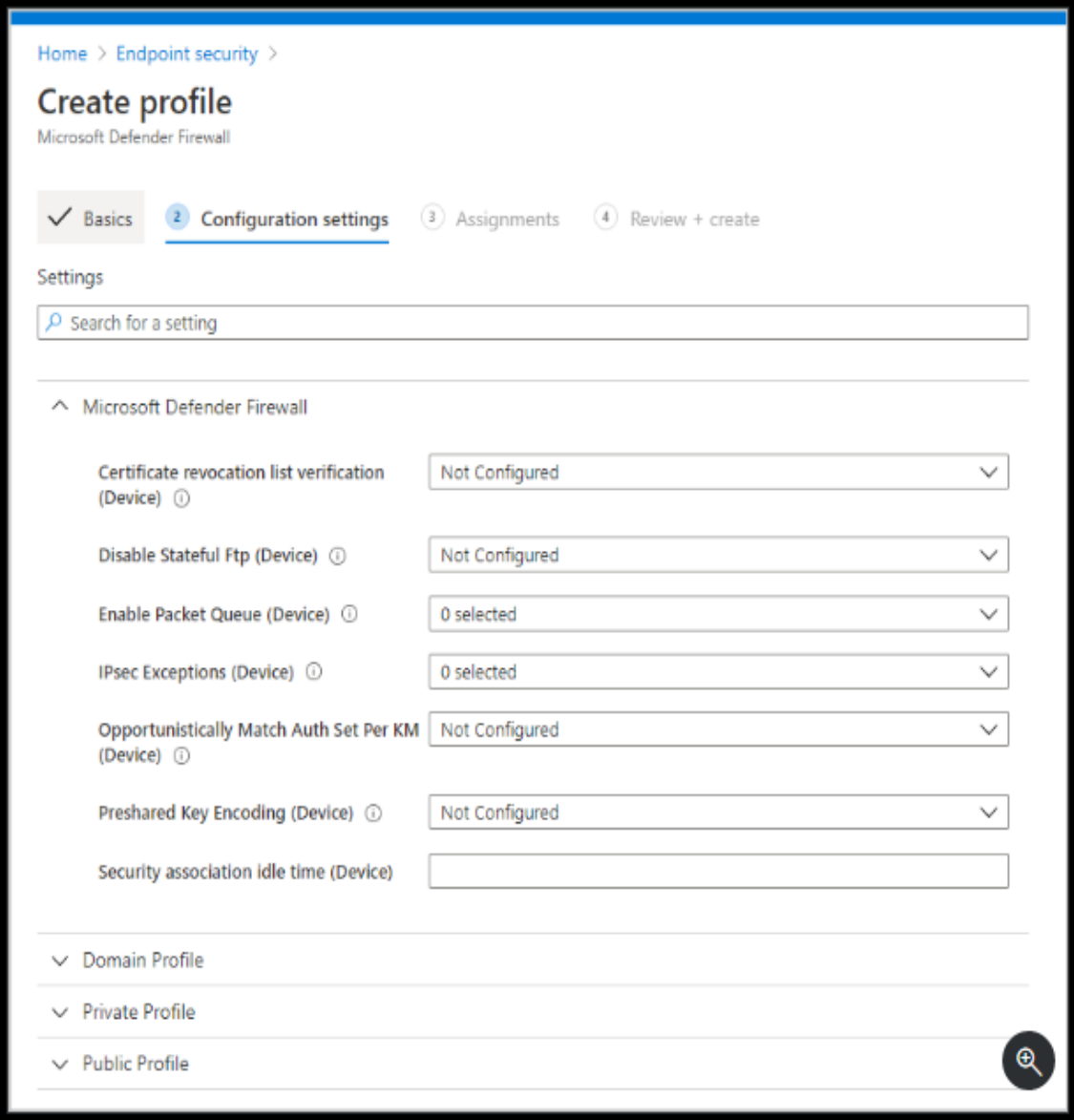
2. Select **Endpoint security** > **Firewall** then **Create Policy.**

3. Create a profile with the following settings:

   - **Platform:** Windows 10 and Windows Server (ConfigMgr)
     - Only Windows 10 clients can be targeted with firewall policies currently.
   - **Profile:** Microsoft Defender Firewall (preview)

4. Select **Create** then give the profile a **Name** and a **Description.**

5. On the **Configuration settings** page, set the firewall settings for the devices.



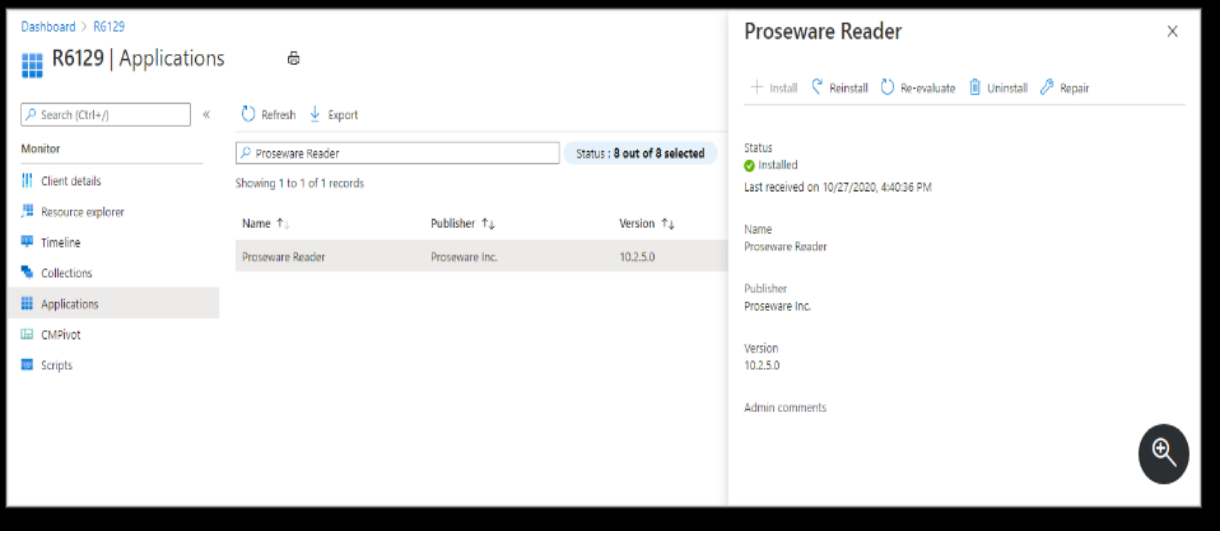
6. On the **Assignments** page, select the collections to include for the policy assignment then choose **Next.**

7. Review the settings on the **Review + Create** page and select **Create** when you're done.

Enhancements to applications in Microsoft Endpoint Manager admin center

We've made improvements to applications for tenant attached devices. Administrators can now do the following actions for applications in the Microsoft Endpoint Manager admin center:

- **Uninstall** an application
- **Repair** installation of an application
- **Re-evaluate** the application installation status
- **Reinstall** an application has replaced **Retry installation**



Improvements to BitLocker management

Based on your UserVoice feedback, you can now manage BitLocker policies and escrow recovery keys over a cloud management gateway (CMG). This change also provides support for BitLocker management via internet-based client management (IBCM) and when you configure the site for enhanced HTTP. There's no change to the setup process for BitLocker management. For more information, see Deploy BitLocker management.

If you have either the Helpdesk or Self-Service portals set up, use these portals to validate that clients escrow their keys directly to a management point. For more information, see Set up BitLocker portals. Continue to use BitLockerManagementHandler.log to help troubleshoot client communication.

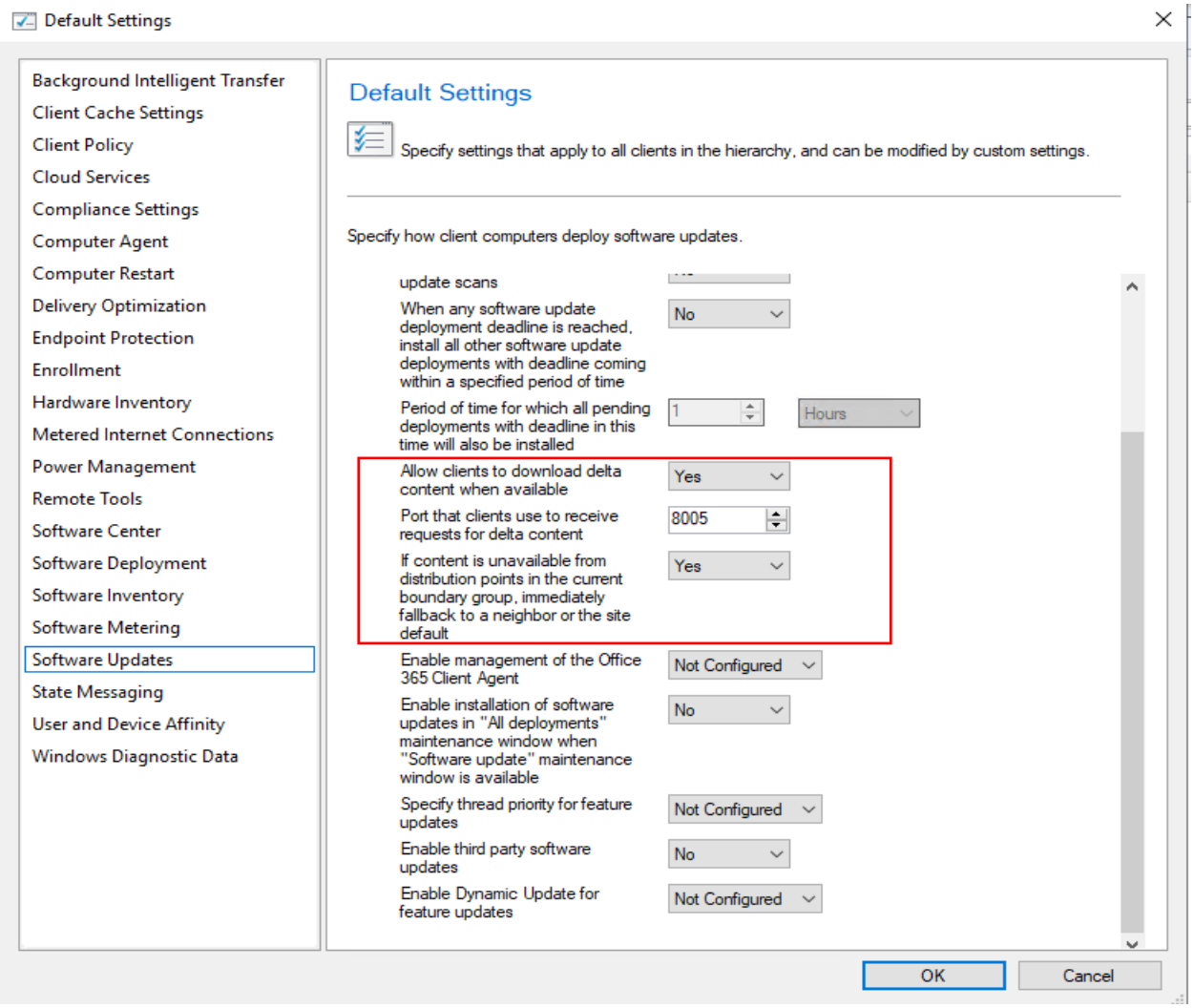
Known issue with BitLocker management

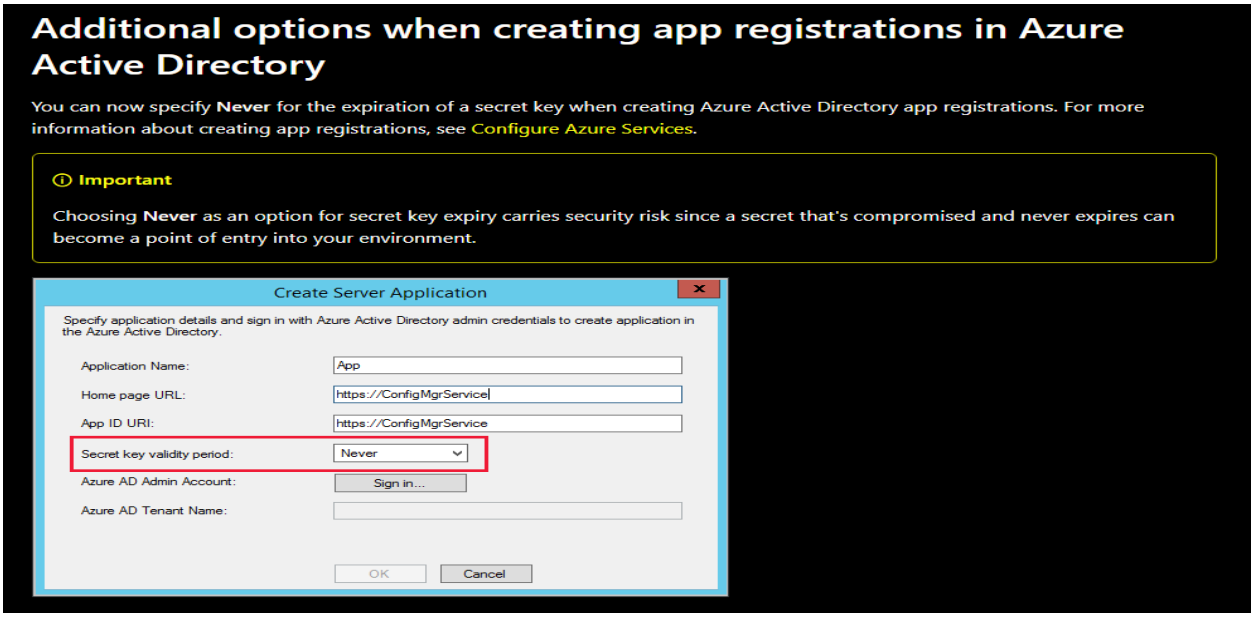
When the client can't communicate with an on-premises management point, there's an issue with the client's BitLocker configuration for key recovery. As a temporary work around for this preview release:

1. Set the following registry key on the client: `HKLM\SOFTWARE\Microsoft\CCM\BLM, "UseKeyRecoveryService"=dword:00000001`
2. Restart the **SMS Agent Host** (ccmexec) service.

This value resets each time the client evaluates the BitLocker management policy, which is seven days by default.

Immediate distribution point fallback for clients downloading software update delta content - There's a new client setting for software updates. If delta content is unavailable from distribution points in the current boundary group, you can allow immediate fallback to a neighbor or the site default boundary group distribution points. This setting is useful when using delta content for software updates since the timeout setting per download job is 5 minutes.





Validate internet access for the service connection point

If you use Desktop Analytics or tenant attach, the service connection point now checks important internet endpoints. These checks help make sure that the cloud-connected services are available. It also helps you troubleshoot issues by quickly determining if network connectivity is a problem.

For more details, review the **EndpointConnectivityCheckWorker.log** file on the service connection point.

A failure isn't always determined by the HTTP status code, but if there's network connectivity to an endpoint. The following scenarios can cause a check to fail:

- Network connection timeout
- SSL/TLS failure
- Unexpected status code:

Status code	Description	Possible reason
407	Proxy authentication required	May indicate a proxy issue
408	Request timeout	May indicate a proxy issue
426	Upgrade required	May indicate a TLS misconfiguration
451	Unavailable for legal reasons	May indicate a proxy issue
502	Bad gateway	May indicate a proxy issue
511	Network authentication required	May indicate a proxy issue
598	Network read timeout error	Not RFC compliant, but used by some proxy servers to indicate a network timeout
599	Network connection timeout error	Not RFC compliant, but used by some proxy servers to indicate a network timeout

Improvements to the administration service

The Configuration Manager REST API, the administration service, requires a secure HTTPS connection. With the previous methods to enable HTTPS, enabling IIS on the SMS Provider was a prerequisite.

Starting in this release, you no longer need to enable IIS on the SMS Provider for the administration service. When you enable the site for enhanced HTTP, it creates a self-signed certificate for the SMS Provider, and automatically binds it without requiring IIS.

If you previously had IIS installed on the SMS Provider, you can remove it. Then restart the SMS_REST_PROVIDER component.

> **Note**
>
> If you don't use enhanced HTTP, you need to manually bind a server authentication certificate to port 443 on the SMS Provider. One method is to use IIS.
>
> You can also use the netsh command line tool, which doesn't require IIS. You can use a command line similar to the following example:
>
> ```
> netsh http add sslcert ippport=<ipaddress>:443 certhash=<certhash>
> ```
>
> You may require additional command line options depending upon your environment and requirements. For more information, see **Netsh http commands**.

This concludes TP 2010.2 install.

Thanks

Ram Lan
31st Oct 2020