Best SCCM CMG Cloud Management Gateway Implementation Guide

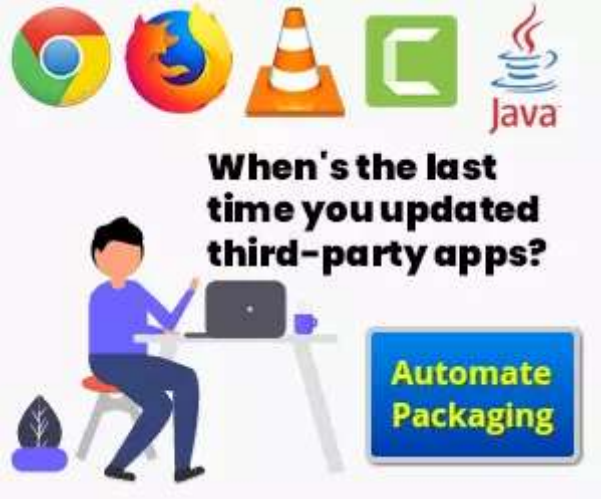
Last Updated: April 12, 2022 by Vimal Das

Let's check the SCCM CMG Cloud Management Gateway Implementation Guide in this post. SCCM Cloud Management Gateway (CMG) architecture and its co-management environment are discussed in Part 1.

In this post, let us consider how to configure SCCM CMG with **fewer certificates** (New SCCM CMG Setup Guide). The option to deploy a Cloud Management Gateway (CMG) as a **cloud service (classic) is deprecated**. All CMG deployments should use a virtual scale set.

The Cloud Management Gateway (CMG) provides a simple way to manage SCCM clients on the internet. The CMG is a PaaS (Platform As A Service) solution in Azure. So, we don't

need to maintain the servers in the Azure platform, unlike Azure IaaS (Infrastructure As A Service) solution.



> The latest version of How To Install SCCM Client Using Intune For Autopilot Provisioned Devices HTMD Blog (anoopcnair.com).

We need to set up and configure Azure Cloud Services within SCCM before implementing Co-Management CMG. Co-Management CMG is not a prerequisite for all the SCCM Co-Management scenarios.

However, CMG is required for the scenario where you want to install an SCCM client from the internet. SCCM **C**loud **M**anagement **G**ateway (**CMG**) & CDP are necessary for the above situation.

- SCCM CMG SCCM Cloud Management Gateway Workflow Scenarios 1
- Download Content Using Cloud Management Gateway

- End-User Experience Of Windows 10 Co-Management
- How To Setup Co-Management – Firewall Ports Proxy Requirements

Introduction – Best SCCM CMG Cloud Management Gateway Implementation Guide

We all know that SCCM CMG is evolving. So, if you are planning SCCM CMG in your environment, Upgrade SCCM to the latest version to have more enhanced features of SCCM CMG.

You can refer to appropriate SCCM versions (SCCM 1810, 1902, and 1906) documentation. CMG has been many improvements (Cloud Management Gateway) with every new SCCM version.

> **NOTE! –** Are you planning to replace **SCCM IBCM servers with SCCM CMG**? I recommend reading the following post, "SCCM IBCM Vs. CMG Differences a Real World Comparison."

Cloud Management gateway Architecture

CMG Architecture *New* **SCCM CMG Setup Guide** – Best SCCM CMG Cloud Management Gateway Implementation Guide 1

1. Internet-connected SCCM client request for policy from Azure CMG cloud service
2. Azure CMG cloud service forwards the client communication to the on-premises CMG connection point. CMG cloud service gets the policy from On-premise MP and SUP through the CMG connection point role.
3. CMG connection point role acts as a proxy and builds a 2-way communication channel between on-premise SCCM (MP & SUP) and Azure CMG cloud service
4. Finally, SCCM clients get policy and content from the Azure CMG cloud service.

Note: CMG supports the management point and software update point roles only. More details about SCCM CMG-supported communications are available **here**.

SCCM CMG Cloud Management Gateway Prerequisite

The following is the quick list of SCCM CMG setup pre-requisites.

- Unique CMG DNS name
- Azure subscription to host CMG
- Azure permission with Global Admin and subscription owner rights.
  - Subscription admin permission to deploy CMG cloud service
  - Global /Service Admin permission to integrate SCCM site with Azure AD using Azure Resource Manager
  - In this post, My ID already had the higher privilege with Global admin rights assigned which were used for all configurations. Hence, I did not have to worry much about these pre-requisites.

- Internet access connectivity requirements
- Network ports requirements
- Windows 10 devices should have IPv4 enabled
- A **server authentication certificate** for the CMG
- Service connection point in online mode. The service connection point is responsible for deploying the CMG in Azure
- On-premises Windows server to host the CMG connection point.

In this post, we host the CMG connection point role on a dedicated server along with MP and SUP with enhanced HTTPS enabled. If you already have HTTPS-enabled MP and SUP, then no need for a separate server.

Microsoft.ClassicCompute & Microsoft. Storage resource providers must be registered within the Azure subscription.

I would recommend reading **CMG Prerequisite** and **Certificate requirements** before implementing Co-Management CMG setup.

7 steps for SCCM Cloud Management Gateway Configuration

SCCM CMG Cloud Management Gateway Implementation Guide.

New **SCCM CMG Setup Guide** SCCM CMG Cloud Management Gateway Implementation Guide

Infrastructure setup used for this post

Let's check the infrastructure components used in the SCCM Cloud Management Gateway setup explained in this post.

- AADconnect enabled hybrid Azure AD join.
- SCCM 1902
- Internal PKI CA for certificates.

In this post, we are not using a third-party certificate.

- Dedicated site server with MP and SUP for CMG
- Windows 10 1903 Enterprise
- Let us cover each configuration step in detail

Verify unique SCCM CMG DNS

In this step, we need to identify the unique CMG service name that we will use later in SCCM. SCCM configures the CMG cloud service in *.cloudapp.net domain. Hence, the CMG service in azure must be unique and not used by anyone.

Note: we do not have to create the CMG service in the portal. SCCM will take care of deploying the CMG cloud service. We need to ensure the CMG service name is unique.

Below are the steps to Check the Unique service name

- Sign in to the Azure portal. Search for **Cloud service**.
- Select **Cloud service and** type the prefix in the **DNS name** field.
- If the domain name is available, the interface reflects green color.

New **SCCM CMG Setup Guide** – Cloud Service -Best SCCM CMG Cloud Management Gateway Implementation Guide

If the Name is unavailable, the interface reflects red color. Try a new name if red.

Best SCCM CMG Cloud Management Gateway Implementation Guide

New **SCCM CMG Setup Guide –** DNS selection for CMG – SCCM CMG Cloud Management Gateway Implementation Guide.

SCCM Cloud management gateway can now serve Cloud distribution points as well. Below are the steps to Check a unique service name for the storage

- Sign in to the Azure portal. Search for a Storage account. Select Create.
- Type the name prefix in the “Storage account **name”** field.
- Green tic state storage name is unique and available.

New **SCCM CMG Setup Guide** – Storage Account -Best SCCM CMG Cloud Management Gateway Implementation Guide 5

Make a note of this unique name. Later while configuring CMG wizard in SCCM, we will use this name.

Step 1 completed 🙂 Let us proceed to the next step.

Certificate preparation – SCCM CMG Cloud Management Gateway Implementation Guide

To configure CMG, we need at least One certificate (Server authentication certificate). Based on the need or scenario, you may need more certificates; we need One certificate only (Server Authenticate in this post or scenario). Let us discuss server-side and client-side certificates.

Server Side certificate

Third-party vendors like DigiCert or Microsoft PKI can issue a Server authentication certificate. Certificate issued by both supported. In this post, we will use Microsoft Enterprise PKI.

The server authentication certificate is mandatory while configuring CMG for any scenario. In part 1 of this post, we discussed different CMG scenarios.

Note: Microsoft recommends using a trusted third-party certificate provider like DigiCert, etc. Windows 10 trusts these third-party certificates without any Root certificate dependency. We will discuss more in later sections.

Let us discuss the steps to get the server authentication certificate.

New **SCCM CMG Setup Guide** – SCCM PKI Cert for SCCM CMG -Best SCCM CMG Cloud Management Gateway Implementation Guide 6

- Step 1: Create a server authentication certificate template.
- Step 2: Enable server authentication certificate template.
- Step 3: Enroll the server authentication certificate.
- Step 4: Export the certificate's private key.
- Step 1 & Step 2 – Configuration is done from CA server.
- Step 3 & Step 4 – Configuration is done from the SCCM server.

Step 1: SCCM CMG Setup Guide – Create server authentication certificate template

Let's learn how to Create a server authentication certificate template for SCCM CMG.

- Log in to the Certification Authority server. Open the Certification Authority console (certsrv. msc).
- Right-click Certificate Templates and select Manage.
- Right click Web Server and click Duplicate Template.

New **SCCM CMG Setup Guide** – Certificate Templates – Best SCCM CMG Cloud Management Gateway Implementation Guide 7

Click on the General tab and modify the display name. Example: Server certificate SCCM CMG.

New **SCCM CMG Setup Guide** – Server Certificate for CMG

Click on the Request Handling tab. Check the box "**Allow private key to be exported**." Click **OK**.

New **SCCM CMG Setup Guide** – Allow Private Key to be Exported – SCCM CMG Cloud Management Gateway Implementation Guide

Click on the Security tab. Add the security group that contains SCCM server computer accounts. Please ensure the group has read and enrolled permission.

By default, the Enterprise admin security group has enrollment permission. Please remove the enterprise admin group from the list.

New **SCCM CMG Setup Guide** – Read Write Access for SCCM CMG Cert

- Close Certificate Template window

Step 2: SCCM CMG Setup Guide – Enable server authentication certificate template

In the previous step, we prepared a certificate template for CMG. However, the certificate template is not enabled. Let us do that now.

Launch Certification Authority console. Right-click Certificate Template and click New > Certificate Template to Issue.

New **SCCM CMG Setup Guide** – Create Template – **Step 2: SCCM CMG Setup – Enable server authentication certificate template**

Select the template we created in step one and click OK to enable. Done.

New **SCCM CMG Setup Guide** – Enable Certificate – SCCM CMG Cloud Management Gateway Implementation Guide

Step 3: SCCM CMG Setup Guide – Enroll the server authentication certificate in SCCM

> **Note**: It is recommended to **reboot the SCCM server** before enrolling in the certificate. This will allow refreshing the SCCM computer authentication token with the CA server. We already provided enrollment permission for the SCCM server in the Certificate template.

- **Launch MMC and Certificates > Local Computer > Personal > Certificates**
- **Right click Certificates > All Task > Request New Certificate**

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Click **next** to continue.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Select the certificate template we issued from CA. Click **more information** to add details.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Under the Subject Name Type drop-down, choose Common Name in the Subject tab.

Enter a unique name, which we already verified in step one. The name should end with ***.cloudapp.net**.

Click **Add** and **OK** to close.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

The certificate enrolled successfully. Click Finish.

Step 4: SCCM CMG Setup Guide – Export the private key

Finally, in this step, we will export the private key (.PFX) for the certificate, which we created in the previous step three. We need this certificate to configure CMG.

Let us go through the steps to export the private key.

- Launch MMC and Certificates > Local Computer > Personal > Certificates
- Right click on XXXXX.cloudapp.net certificate > All Tasks > Export

SCCM CMG Cloud Management Gateway Implementation Guide

In the wizard, choose “Yes” and export the private key. Leave everything as default and secure the certificate with a password. Save the certificate with.PFX extension to finish the wizard.

SCCM CMG Cloud Management Gateway Implementation Guide

SCCM CMG Setup Guide – Client-Side certificate

Why is a certificate required on the Windows 10 or Windows 11 client for CMG?

SCCM client must authenticate to confirm its identity before communication with CMG cloud. There are three options for authentication. In this post, we will use 3rd option.

1. PKI client authentication certificate or
2. User identity token (Azure AD user discovery) or
3. Azure AD computer identity (Using Default Azure client Auth certificate)

By default, Hybrid or Azure only joined computers will receive below two certificates from Azure. These certificates can serve as an authentication token for CMG service. In this post, we are using these two certificates.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Note 1: if we use Microsoft internal PKI, then Root CA of your internal PKI CA is required on the Windows 10 client.

Note 2: if you are using third-party certificates like Entrust, user trust, that, DigiCert, etc., then Root CA is not required. You do not need any roo even for Azure AD connected machines CA even for Azure AD connected machines. Unlike Microsoft enterprise PKI, Windows 10 trusts third-party certificates without any need for root CA. This reduces the complexity and root CA dependency on the client-side. Microsoft recommends third-party certifications because of this rationale.

Azure Service integration with SCCM | SCCM CMG Setup Guide

In this step, we will integrate SCCM with Azure cloud services. This integration was performed using the SCCM Azure Services Wizard. For more configuration details on Azure Services wizard, refer here.

This wizard can configure two things.

- **Azure AD web app registration**: SCCM clients use Azure web app URLs to authenticate with Azure.
- **Azure AD user discovers** (optional): We are not going to configure. We discussed already that in this post User identity token is not used for authentication
- Navigate to Administration > Overview > Cloud Services > Azure Services.
- Right-click Azure Services and click Configure Azure Services.

New **SCCM CMG Setup Guide** – Best SCCM CMG Cloud Management Gateway Implementation Guide

Select "**Cloud Management**"

New **SCCM CMG Setup Guide** – Cloud Services – Best SCCM CMG Cloud Management Gateway Implementation Guide

In the below wizard, we have to configure Webapps. Check with your azure administrator before deciding whether you can use existing web apps or new webapps for CMG.

You have two options. In this guide, we use the second option.

(1) Pre-create the Azure webapps manually and import them in the below SCCM wizard. For more details about the configuration, refer here.
(2) SCCM creates the Web app automatically in Azure.

You are signed in with a Subscription Admin and select the default web URL.

New **SCCM CMG Setup Guide** – Server App – SCCM CMG Cloud Management Gateway Implementation Guide

After Successful sign in, Server and Client web app details get populated automatically. Click **Next**.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

- For more details about the web app's configuration and workflow refer here.
- Next, you will see the below wizard enable Azure user discovery.

In this post, we are not enabling user discovery. Let us discuss why we are not enabling. There are two reasons.

(1) Authentication: The SCCM client uses computer identity (using certificate) for CMG authentication in this post. Therefore, we do not need a user token for authentication identity.

2) Deployment: In my scenario, SCCM deployments will be device-based instead of user-based. However, you can consider enabling user discovery if that is not the case for you.

New **SCCM CMG Setup Guide** – Discovery SCCM CMG Cloud Management Gateway Implementation Guide

Click next and Close on the Completion page.

Verify the Azure service integration | Best SCCM CMG Cloud Management Gateway Implementation Guide

You will see two new web app registrations in the Azure console. These web apps registrations indicate successful Azure service integration. Go to Home > App registrations. Check for the client and server apps name we configured in the SCCM console.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

CMG deployment configuration in SCCM

We have done a lot of prep work. Finally, we reached the step to deploy the CMG service in Azure using the SCCM console. While configuring CMG cloud service, please ensure CMG is configured at the top-tier site of the SCCM hierarchy.

- On the ConfigMgr Console, go to **Administration > Cloud Services > Cloud Management Gateway**.
- Click Create Cloud Management Gateway on the ribbon menu.

New **SCCM CMG Setup Guide** – Best SCCM CMG Cloud Management Gateway Implementation Guide 8

Sign In with the Azure Subscription Admin account The subscription info, the Web App details, and tenant details will auto-populate. We already created the webapps in step 3 as Azure service integration.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Browse and select the Server authentication certificate that we exported in step two.

The CMG service name will auto-populate from the certificate we provided while importing the certificate in Step 2. The CMG Service name will populate with the XXXX.cloudapp.net domain name.

> **Note**: CNAME is required if you are using the custom domain name. You have to create a CNAME record in public DNS pointing to

Select the Region – The Azure region where the cloud service to host. For the China region, I would recommend checking with Microsoft.

- Select the option new resource group.
- Select the group from the drop-down menu.

Choose the number of VM Instances. The maximum VM instance value you can provide is 16. Each standard VM A2 hosted in Azure can support approx 6000 clients. In addition, 2000 simultaneous connections.

> In production, consider multiple VM for redundancy or availability. You can add "instance" to the existing CMG, which can be done simply by adding another VM. There is no need to have an additional CMG cloud service for HA because the Azure CMG cloud service is already on HA.

Un-check "**Verify Client Certificate Revocation**." In our scenario, we are not using a PKI client authentication certificate, so this setting is not relevant to us. Clear this if you have not published the CRL on the internet. Recommended checking with your security or PKI team.

Since we are using Internal CA Cert for CMG, upload respective Root and Intermediate certificates.

Enable the CMG to serve as a cloud distribution point as well.

- Click **Next** to proceed and configure the **CMG cloud service.**

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

On the Alerts page, select default and click **next**. On the completion page, click **Close**.

Verify the CLOUD MANAGEMENT GATEWAY deployment

There are three areas to monitor the CMG service deployment. SCCM CMG Cloud Management Gateway Implementation Guide.

1. SCCM Console
2. Logs
3. Azure Resource

SCCM console:

Navigate to **Administration->cloud services->cloud management gateway.** Initially, the status will show as "Provisioning."

New **SCCM CMG Setup Guide** – Provisioning – SCCM CMG Cloud Management Gateway Implementation Guide

After approx. **15 minutes**, the status changed to Provisioning Completed **– > Ready**.

New **SCCM CMG Setup Guide** – SCCM CMG is Ready – SCCM CMG Cloud Management Gateway Implementation Guide

SCCM logs related Cloud Management Gateway Setup

Open **CloudMgr.log** and CMGSetup.log to view the status. SCCM service connection point is responsible for deploying the CMG service in Azure. Let us cover more details about the logs, events, and troubleshooting in the next post.

Azure Resource deployment monitoring:

Log in to the Azure Console and navigate to the resource group we created. You will see whether a cloud service and storage account are made.

New **SCCM CMG Setup Guide** – Logs SCCM CMG Cloud Management Gateway Implementation Guide

We can monitor the CMG deployment activity from the Azure console. Navigate to Azure->monitor–>Activity log

New **SCCM CMG Setup Guide** – Logs from Azure – SCCM CMG Cloud Management Gateway Implementation Guide

You can also monitor the resource group activity by selecting the resource group you created from the SCCM console.

New **SCCM CMG Setup Guide** – SCCM CMG Activity Log – SCCM CMG Cloud Management Gateway Implementation Guide

Install CMG connection point role | SCCM CMG Setup Guide

In previous step four, we deployed the CMG cloud service. This step will install the CMG connection point SCCM role on-premise and connect with the CMG cloud service.

The CMG connection point role can be installed on the remote Site System server with or without MP/SUP rode; I have a dedicated CMG role with MP and SUP enabled for H in this guide. Ensure internet proxy allows CMG connection point communication with CMG cloud service.

> **Note 1:** multiple CMG connection point role installed servers can communicate with a single CMG cloud service.
> **Note 2:** it is also possible to create multiple CMG cloud services and connect with various CMG connection point role servers.

The benefit of having multiple CMG connection point roles is load balancing of client traffic from the CMG cloud service to the on-premise MP/SUP. Refer here for more details on planning the CMG in SCCM hierarchy design.

- Let us go through the steps to configure the CMG role.In the SCCM console, go to Administration > Site Configuration > Servers and Site System Roles.
- Right-click the site server to Add Site System Roles.
- In this post scenario, the CMG connection role is installed on a dedicated remote server.
- Provide the remote site server name .

New **SCCM CMG Setup Guide** – Add Role – SCCM CMG Cloud Management Gateway Implementation Guide

Check the box for **Cloud Management gateway connection point**. Click **Next**.

New **SCCM CMG Setup Guide** SCCM CMG Cloud Management Gateway Implementation Guide

You link the on-premise CMG site server role to its appropriate CMG cloud service in the below step. Select the Cloud management service from the drop-down menu if you have multiple CMG cloud services.

NOTE! – SCCM CMG cloud service region populates automatically.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Note: The CMG connection point role from a site can only connect to one CMG cloud service, as shown above. For redundancy or scalability, adding a multiple “instance” to the CMG clouse se is possiblerver, which is adding another VM. We discussed this in step 4. For more details, refer here.

Click next and ok to complete the wizard.

How to Verify the CMG role setup

THE CONSOLE WILL SHOW the CMG cloud service, region, and associated on-premise Connection Point server.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Note: You will also be charged based on outbound data transfer. For more details, refer here.

Verify the CMG Role installation

After successful CMG role installation, you can see the CMG role start establishing a connection with CMG cloud service (*.cloudapp.net). For more details about this component activity, refer to log – **CMGService.log** and **SMS_Cloud_ProxyConnector.log**.

Read More about SCCM Logs.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

After a few minutes, we will see CMG's on-premise role connect with CMG cloud service and start communication. In the next post part 3, we will detail **troubleshooting and events**.

New **SCCM CMG Setup Guide** – Best SCCM CMG Cloud Management Gateway Implementation Guide 11

SCCM CMG Site system & MP settings

In this step, let us enable component roles (MP/SUP) and the site system to respond to CMG requests. With this configuration, SCCM clients from the internet communicate with on-premise MP and SUP through CMG cloud service. I dedicated a remote SCCM server with MP, and the SUP role enabled CMG communication in this post only.

Note: CMG supports only two roles: SUP and MP

Enable the MP for CMG – SCCM CMG Cloud Management Gateway Implementation Guide

Navigate to Administration > Site Configuration > **Servers and Site System Roles**.

Select the Site Server holding the MP role (planned for dedicated CMG communications).

Check the box "**Allow Configuration Manager cloud management gateway traffic on the Management Point Properties**."

Change the connection to "**Allow Internet-only connections**." Because in my setup, there is a dedicated MP server for CMG. Also, want to ensure only internet-connected SCCM client requests communicate to the dedicated MP.

New **SCCM CMG Setup Guide** – Best SCCM CMG Cloud Management Gateway Implementation Guide 12

It is important to understand different MP client connection modes and design accordingly. For more details, refer here.

Enable the SUP for CMG – SCCM CMG Cloud Management Gateway Implementation Guide

Select the Site Server holding the SUP role (planned for dedicated CMG communications). Under Software update point properties, check the "Allow Configuration Manager cloud management gateway traffic" box.

Click OK. Change the client connection type to “allow internet-only connections.” Because in my scenario, there is a dedicated SUP server for CMG. Also, want to ensure only internet-connected SCCM client requests communicate to the SUP.

New **SCCM CMG Setup Guide** – SCCM CMG Cloud Management Gateway Implementation Guide

Site system settings for SCCM CMG

Navigate to Site Properties > Client Computer Communication tab. Check the box “**Use Configuration Manager-generated certificates for HTTP site systems**.”

The other client computer settings are left unchecked because we are not using PKI client authentication. Instead, a cloud-based device identity is used to authenticate with the CMG and management point.

New **SCCM CMG Setup Guide** – SCCM EHTTP Certs – SCCM CMG Cloud Management Gateway Implementation Guide

NOTE – SCCM EHTTP = Certificates are SCCM Self signed certificates which can replace some of the PKI certificate requirements. More details https://docs.microsoft.com/en-us/sccm/core/plan-design/hierarchy/enhanced-http

Client Agent Setting for SCCM CMG

Creating a custom SCCM client agent setting is recommended to enable CMG instead of Default client settings. Custom client agent settings provide better control. You can use SCCM collection and custom SCCM client agent setting to restrict the number of clients to use the CMG.

- Go to Administration / **Client Settings**.
- Click Create Custom **Client Device Settings** on the top ribbon and select cloud services.
- In the custom client agent settings, enable the option "**enable clients to use a cloud management gateway**."
- Enable "**Allow access to the cloud distribution point**."

New **SCCM CMG Setup Guide** – *SCCM Client Settings* – Best SCCM CMG Cloud Management Gateway Implementation Guide 13

End Result – SCCM CMG Cloud Management Gateway Implementation Guide

Finally, you can monitor CMG's overall status, including the total no of CMG requests, full request size, concurrent connections, etc.

New **SCCM CMG Setup Guide** – *END Results* – SCCM CMG Cloud Management Gateway Implementation Guide

In the SCCM client, you will see the URL in the control panel. This indicates your SCCM client received CMG URL details. When your computer moves to the internet, it will get a policy from CMG cloud service and content from cloud DP.

New **SCCM CMG Setup Guide** – *SCCM EHTTP Certs* End Result – SCCM CMG Cloud Management Gateway Implementation Guide

In the next post, let us discuss the workflow on the client-side and troubleshooting.

Thank you, Rajul, for your input.

Resources

- Plan for the cloud management gateway in SCCM
- End-User Experience of Windows 10 Co-Management
- Multiple Pilot Groups SCCM co-Management Workloads

Author

Vimal has more than 10 years of experience in SCCM device management solutions. His main focus is on Device Management technologies like Microsoft Intune, ConfigMgr (SCCM), OS Deployment, Patch Management. He writes about the technologies like SCCM, Windows 10, Microsoft Intune, and MDT.

SCCM

Search..... Search