200 XP

Explore Windows Admin Center

10 minutes

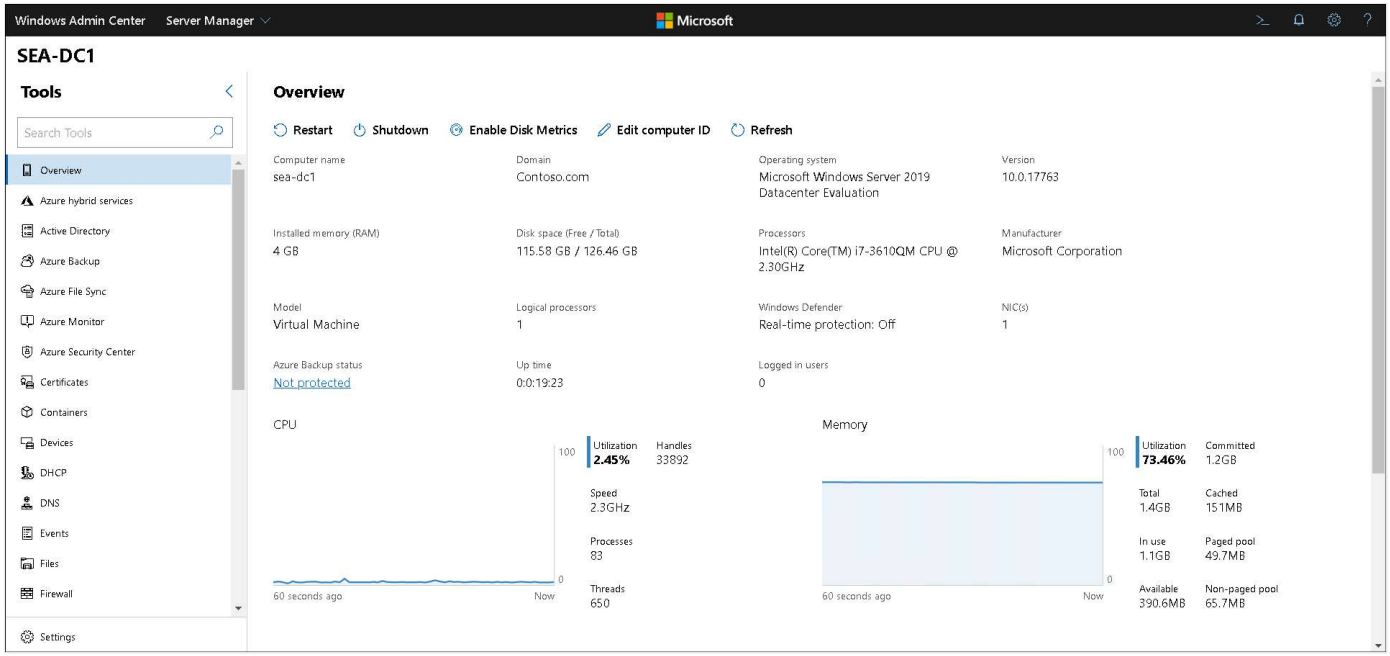
As a senior Windows Server administrator at Contoso, you're responsible for planning a new approach to performing server administration. In the past, managing and administrating the IT environment involved using different tools across multiple consoles. Windows Admin Center combines those tools into a single console that can easily be deployed and accessed through a web interface. You decide to investigate Windows Admin Center.

Overview

Windows Admin Center is a modular web application comprised of the following four modules:

- Server manager
- Failover clusters
- Hyper-converged clusters
- Windows 10 clients

> **Note**
>
> Windows Admin Center manages servers that run Windows Server 2008 R2 and newer. If you want to manage servers other than the local server, you must add those other servers to the console.



Windows Admin Center has two main components:

- Gateway. The Gateway manages servers through PowerShell remoting and Windows Management Instrumentation (WMI) over Windows Remote Management (WINRM).
- Web server. The Web server component observes HTTPS requests and serves the user interface to the web browser on the management station. This is not a full install of Internet Information Services (IIS), but a mini Web server for this specific purpose.

> **Important**
>
> Because Windows Admin Center is a web-based tool that uses HTTPS, it requires a X.509 certificate to provide SSL encryption. The installation wizard gives you the option to either use a self-signed certificate or provide your own SSL certificate. The self-signed certificate expires 60 days after it is created.

Benefits of Windows Admin Center

The following table describes the benefits of Windows Admin Center:

Expand table

Benefit	Description
Easy to install and use	You can download and install it on Windows 10 or Windows Server through a single Windows Installer (MSI) and access it from a supported web browser.
Compliments existing solutions	It does not replace but compliments existing solutions such as Remote Server Administration Tools, System Center, and Azure Monitor.
Manage from the internet	It can be securely published to the public internet so you can connect to and manage servers from anywhere.
Enhanced security	Role-based access control lets you fine-tune which administrators have access to which management features. Gateway authentication provides support for local groups, Active Directory groups, and Microsoft Entra groups.
Azure integration	You can easily get to the proper tool within Windows Admin Center, then launch it to the Azure portal for full management of Azure services.
Extensibility	A Software Development Kit (SDK) will allow Microsoft and other partners to develop new tools and solutions for more products.
No external dependencies	Windows Admin Center doesn't require internet access or Microsoft Azure. There is no requirement for IIS or SQL server and there are no agents to deploy. The only dependency is to the requirement of Windows Management Framework 5.1 on managed servers.

Supported platforms and browsers

You can install Windows Admin Center on Windows 10 and Windows Server.

> ⓘ **Important**
>
> Windows Admin Center is not supported on domain controllers and will return an error if you try to install it.

After downloading and installing Windows Admin Center, you must enable TCP port 6516 on the local firewall.

> **Note**
>
> You are prompted to select a TCP port during setup.

The Windows browser versions of Microsoft Edge on Windows 10 and Google Chrome are tested and supported on Windows 10. Other modern web browsers have not been tested and are not officially supported.

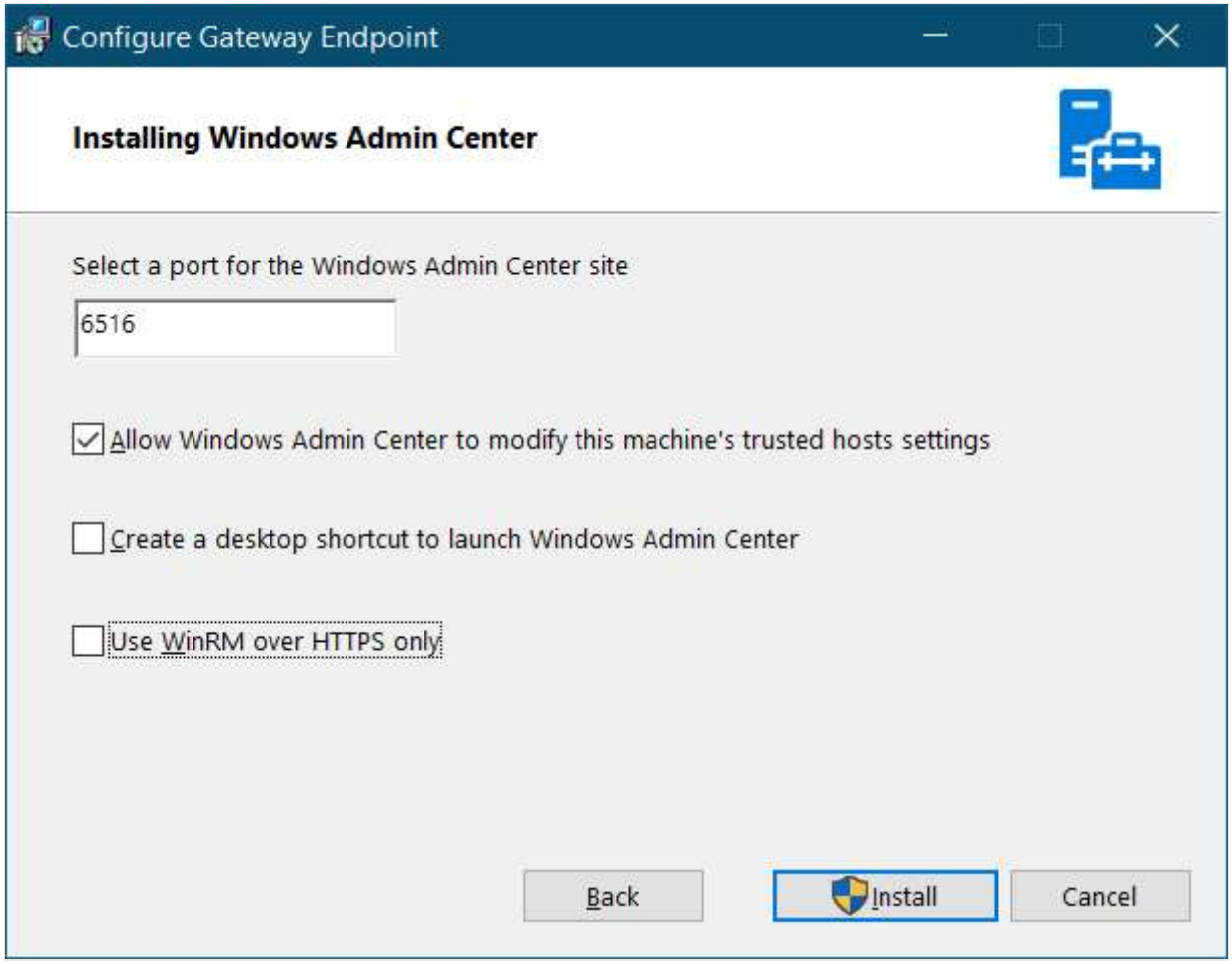
> **Important**
>
> Internet Explorer is not supported and will return an error if you attempt to launch Windows Admin Center.

Authenticate to remote computers

When you connect to a remote computer, you must authenticate to that computer. If the computer you want to manage is part of the same AD DS (Active Directory Domain Services) forest, Kerberos authentication is used.

Where this is not the case, you must configure the target computers as trusted hosts. For example, if you use a workgroup computer installed with Windows Admin Center to administer your domain controllers.

> **Important**
>
> When you install Windows Admin Center on a workgroup computer, you are prompted to allow Windows Admin Center to manage the local computer's TrustedHosts setting. If you bypass this automated setting, you must configure TrustedHosts manually.



You can configure trusted hosts settings by using the following Windows PowerShell command in an elevated Windows PowerShell window. You can specify the remote hosts by IP, FQDN, or NetBIOS name.

PowerShell

```
Set-Item WSMan:localhost\Client\TrustedHosts -Value 'SEA-DC1.Contoso.com'
```

Tip

You can also use a wildcard setting: `Set-Item WSMan:\localhost\Client\TrustedHosts -Value '*'`

Demonstration

The following video demonstrates how to administer Windows Server by using Windows Admin Center. The main steps in the process are:

1. Install the Windows Admin Center from a downloadable .msi installer file.
2. Verify that appropriate TCP port is configured during installation.
3. Open **Microsoft Edge** and open **Windows Admin Center**.
4. Add a domain controller to Windows Admin Center.
5. Review the options available on the **Overview** and **Tools** panes.
6. Review the following: Certificates, Performance Monitoring, Processes, Registry, Roles & Features, Scheduled Tasks, and PowerShell.

Quick review

1. Using Windows Admin Center, an administrator connects to the domain controller, SEA-DC1. The administrator wants to add a new user account to the Contoso.com AD DS domain. Which of the following procedures would *not* work? *

- ◯ In Windows Admin Center, connect to SEA-DC1 and then, in the navigation pane, select **Active Directory**. Select **Create**, then select **User**. Enter the required details and then select **Create**.
- ◯ In Windows Admin Center, connect to SEA-DC1 and then, in the navigation pane, select **Local users & groups**. Select **Create**, then select **User**. Enter the required details and then select **Create**.
- ◯ In Windows Admin Center, connect to SEA-DC1 and then, in the navigation pane, select **PowerShell**. After signing in, use the **New-ADUser** cmdlet to create a new user.

Check your answers