

Document title: Enable-ExchangeCertificate (ExchangePowerShell) | Microsoft Learn

Capture URL: <https://learn.microsoft.com/en-us/powershell/module/exchange/enable-exchangecertificate?view=exchange-ps>

Page loaded at (UTC): Wed, 08 May 2024 13:30:07 GMT

Capture timestamp (UTC): Wed, 08 May 2024 13:30:09 GMT

Capture tool: 2.58.2

Collection server IP: 52.5.8.50

Browser engine: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/121.0.6167.85 Safari/537.36

Operating system: linux x64 (Node v20.5.1)

PDF length: 10

Capture ID: 25yCzoNTy7RFzBmLTkuVHT

User: automation@page-vaul

PDF REFERENCE #: bwsaFTyTYrhG62U3QxWARL



Version

Exchange PowerShell

Search

ExchangePowerShell

Commands

- active-directory
- antispam-antimalware
- client-access
- client-access-servers
- database-availability-groups
- defender-for-office-365
- devices
- email-addresses-and-address-books

encryption-and-certificates

Commands

Enable-ExchangeCertificate

- Export-ExchangeCertificate
- Get-DataEncryptionPolicy
- Get-ExchangeCertificate
- Get-IRMConfiguration
- Get-M365DataAtRestEncryptionPolicy
- Get-M365DataAtRestEncryptionPolicyAssignment
- Get-MailboxIRMAccess
- Get-OMEConfiguration
- Get-OMessageStatus
- Get-RMSTemplate
- Get-SmimeConfig
- Import-ExchangeCertificate
- New-DataEncryptionPolicy
- New-ExchangeCertificate
- New-M365DataAtRestEncryptionPolicy

Download PDF

ExchangePowerShell / encryption-and-certificates



Enable-ExchangeCertificate

Reference

Feedback

Module: ExchangePowerShell

Applies to: Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

This cmdlet is available only in on-premises Exchange.

Use the Enable-ExchangeCertificate cmdlet to enable an existing certificate on the Exchange server for Exchange services such as Internet Information Services (IIS), SMTP, POP, IMAP and Unified Messaging (UM). Once you enable a certificate for a service, you can't disable it.

To see the existing certificates that are used for Exchange services, use [Get-ExchangeCertificate](#).

For information about the parameter sets in the Syntax section below, see [Exchange cmdlet syntax](#).

In this article

Syntax

- Description
- Examples
- Parameters
- Inputs
- Outputs

Syntax

PowerShell

Copy

```
Enable-ExchangeCertificate
  [-Thumbprint] <String>
  [-Services <AllowedServices>]
  [-Confirm]
  [-DomainController <Fqdn>]
  [-DoNotRequireSsl]
  [-Force]
  [-NetworkServiceAllowed]
  [-Server <ServerIdParameter>]
  [-WhatIf]
  [<CommonParameters>]
```

PowerShell

Copy

```
Enable-ExchangeCertificate
  [[-Identity] <ExchangeCertificateIdParameter>]
  [-Services <AllowedServices>]
  [-Confirm]
  [-DomainController <Fqdn>]
  [-DoNotRequireSsl]
  [-Force]
  [-NetworkServiceAllowed]
  [-WhatIf]
  [<CommonParameters>]
```

New-DataEncryptionPolicy
New-ExchangeCertificate
New-
M365DataAtRestEncryptionPolic

 Download PDF

```
[[-Identity] <ExchangeCertificateIdParameter>]  
-Services <AllowedServices>  
[-Confirm]  
[-DomainController <Fqdn>]  
[-DoNotRequireSsl]  
[-Force]  
[-NetworkServiceAllowed]  
[-WhatIf]  
[<CommonParameters>]
```

Description

The Enable-ExchangeCertificate cmdlet enables certificates by updating the metadata that's stored with the certificate. To enable an existing certificate to work with additional Exchange services, use this cmdlet to specify the services.

After you run the Enable-ExchangeCertificate cmdlet, you might need to restart Internet Information Services (IIS). In some scenarios, Exchange might continue to use the previous certificate for encrypting and decrypting the cookie that's used for Outlook on the web (formerly known as Outlook Web App) authentication. We recommend restarting IIS in environments that use Layer 4 load balancing.

There are many factors to consider when you configure certificates for Transport Layer Security (TLS) and Secure Sockets Layer (SSL) services. You need to understand how these factors might affect your overall configuration. For more information, see [Digital certificates and encryption in Exchange Server](#).

Secure Sockets Layer (SSL) is being replaced by Transport Layer Security (TLS) as the protocol that's used to encrypt data sent between computer systems. They're so closely related that the terms "SSL" and "TLS" (without versions) are often used interchangeably. Because of this similarity, references to "SSL" in Exchange topics, the Exchange admin center, and the Exchange Management Shell have often been used to encompass both the SSL and TLS protocols. Typically, "SSL" refers to the actual SSL protocol only when a version is also provided (for example, SSL 3.0). For more information, see [Exchange Server TLS configuration best practices](#).

You need to be assigned permissions before you can run this cmdlet. Although this topic lists all parameters for the cmdlet, you may not have access to some parameters if they're not included in the permissions assigned to you. To find the permissions required to run any cmdlet or parameter in your organization, see [Find the permissions required to run any Exchange cmdlet](#).

Examples

Example 1

PowerShell

 Copy

```
Enable-ExchangeCertificate -Thumbprint 5113ae0233a72fccb75b1d01f
```

This example enables a certificate for POP, IMAP, SMTP and IIS services.

Parameters

```
Enable-ExchangeCertificate -Thumbprint 5113ae0233a72fccb75b1d019
```

This example enables a certificate for POP, IMAP, SMTP and IIS services.

Parameters

-Confirm

The Confirm switch specifies whether to show or hide the confirmation prompt. How this switch affects the cmdlet depends on if the cmdlet requires confirmation before proceeding.

- Destructive cmdlets (for example, Remove-* cmdlets) have a built-in pause that forces you to acknowledge the command before proceeding. For these cmdlets, you can skip the confirmation prompt by using this exact syntax: `-Confirm:$false`.
- Most other cmdlets (for example, New-* and Set-* cmdlets) don't have a built-in pause. For these cmdlets, specifying the Confirm switch without a value introduces a pause that forces you acknowledge the command before proceeding.

 Expand table

Type:	SwitchParameter
Aliases:	cf
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-DomainController

The DomainController parameter specifies the domain controller that's used by this cmdlet to read data from or write data to Active Directory. You identify the domain controller by its fully qualified domain name (FQDN). For example, dc01.contoso.com.

The DomainController parameter isn't supported on Edge Transport servers. An Edge Transport server uses the local instance of Active Directory Lightweight Directory Services (AD LDS) to read and write data.

 Expand table

Type:	Fqdn
Position:	Named
Default value:	None

 Expand table

Type:	Fqdn
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-DoNotRequireSsl

The DoNotRequireSsl switch prevents the command from enabling the "require SSL" setting on the default web site when you enable the certificate for IIS. You don't need to specify a value with this switch.

If you don't use this switch, and you use the Services parameter to enable the certificate for IIS, the command enables the "require SSL" setting for the default web site in IIS.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-Force

The Force switch hides warning or confirmation messages. You don't need to specify a value with this switch.

You can use this switch to run tasks programmatically where prompting for administrative input is inappropriate.

By default, when you enable a certificate for SMTP, the command prompts you to replace the existing certificate that's enabled for SMTP, which is likely the default Exchange self-signed certificate.

 Expand table

Type:	SwitchParameter
Position:	Named

you to replace the existing certificate that's enabled for SMTP, which is likely the default Exchange self-signed certificate.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-Identity

The Identity parameter specifies the certificate that you want to configure. Valid values are:

- `ServerNameOrFQDN\Thumbprint`
- `Thumbprint`

You can find the thumbprint value by using the `Get-ExchangeCertificate` cmdlet.

You can't use this parameter with the `Server` parameter.

The `Thumbprint` parameter, not the `Identity` parameter, is the positional parameter for this cmdlet. Therefore, when you specify a thumbprint value by itself, the command uses that value for the `Thumbprint` parameter.

 Expand table

Type:	ExchangeCertificateIdParameter
Position:	1
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-NetworkServiceAllowed

The `NetworkServiceAllowed` switch gives the built-in Network Service account permission to read the certificate's private key without enabling the certificate for SMTP. You don't need to specify a value with this switch.

 Expand table

--

The NetworkServiceAllowed switch gives the built-in Network Service account permission to read the certificate's private key without enabling the certificate for SMTP. You don't need to specify a value with this switch.

 Expand table

Type:	SwitchParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-Server

The Server parameter specifies the Exchange server where you want to run this command. You can use any value that uniquely identifies the server. For example:

- Name
- FQDN
- Distinguished name (DN)
- Exchange Legacy DN

If you don't use this parameter, the command is run on the local server.

You can't use this parameter with the Identity parameter, but you can use it with the Thumbprint parameter.

 Expand table

Type:	ServerIdParameter
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-Services

The Services parameter specifies the Exchange services that the certificate is enabled for. Valid values are:

- Federation: Don't use this command to enable a certificate for

-Services

The Services parameter specifies the Exchange services that the certificate is enabled for. Valid values are:

- Federation: Don't use this command to enable a certificate for federation. Creating or modifying a federation trust enables or modifies how certificates are used for federation. You manage the certificates that used for federation trusts with the New-FederationTrust and Set-FederationTrust cmdlets.
- IIS: By default, when you enable a certificate for IIS, the "require SSL" setting is configured on the default web site in IIS. To prevent this change, use the DoNotRequireSsl switch.
- IMAP: Don't enable a wildcard certificate for the IMAP4 service. Instead, use the Set-ImapSettings cmdlet to configure the FQDN that clients use to connect to the IMAP4 service.
- POP: Don't enable a wildcard certificate for the POP3 service. Instead, use the Set-PopSettings cmdlet to configure the FQDN that clients use to connect to the POP3 service.
- SMTP: When you enable a certificate for SMTP, you're prompted to replace the default Exchange self-signed certificate that's used to encrypt SMTP traffic between internal Exchange. Typically, you don't need to replace the default certificate with a certificate from a commercial CA for the purpose of encrypting internal SMTP traffic. If you want to replace the default certificate without the confirmation prompt, use the Force switch.
- UM: You can only enable a certificate for the UM service when the UMStartupMode parameter on the Set-UMService cmdlet is set to TLS or Dual. If the UMStartupMode parameter is set to the default value TCP, you can't enable the certificate for the UM service.
- UMCallRouter: You can only enable a certificate for the UM Call Router service when the UMStartupMode parameter on the Set-UMCallRouterService cmdlet is set to TLS or Dual. If the UMStartupMode parameter is set to the default value TCP, you can't enable the certificate for the UM Call Router service.

You can specify multiple values separated by commas.

The values that you specify with this parameter are additive. When you enable a certificate for one or more services, any existing services remain in the Services property and you can't remove the existing services. Instead, configure another certificate for the services and then remove the certificate that you don't want to use.

Different services have different certificate requirements. For example, some services may require a server name in the certificate's Subject Name or Subject Alternative Name fields, but other services may require an FQDN. Verify that the certificate supports the services that you want to configure.

 Expand table

Type:	AllowedServices
Position:	Named
Default value:	None
Required:	True

 Expand table

Type:	AllowedServices
Position:	Named
Default value:	None
Required:	True
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-Thumbprint

The Thumbprint parameter specifies the certificate that you want to configure. You can find the thumbprint value by using the Get-ExchangeCertificate cmdlet.

The Thumbprint parameter, not the Identity parameter, is the positional parameter for this cmdlet. Therefore, when you specify a thumbprint value by itself, the command uses that value for the Thumbprint parameter.

 Expand table

Type:	String
Position:	1
Default value:	None
Required:	True
Accept pipeline input:	True
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

-WhatIf

The WhatIf switch simulates the actions of the command. You can use this switch to view the changes that would occur without actually applying those changes. You don't need to specify a value with this switch.

 Expand table

Type:	SwitchParameter
Aliases:	wi
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False

changes. You don't need to specify a value with this switch.

 Expand table

Type:	SwitchParameter
Aliases:	wi
Position:	Named
Default value:	None
Required:	False
Accept pipeline input:	False
Accept wildcard characters:	False
Applies to:	Exchange Server 2010, Exchange Server 2013, Exchange Server 2016, Exchange Server 2019

Inputs

Input types

To see the input types that this cmdlet accepts, see [Cmdlet Input and Output Types](#). If the Input Type field for a cmdlet is blank, the cmdlet doesn't accept input data.

Outputs

Output types

To see the return types, which are also known as output types, that this cmdlet accepts, see [Cmdlet Input and Output Types](#). If the Output Type field is blank, the cmdlet doesn't return data.

Feedback

Was this page helpful?

 Yes

 No

[Provide product feedback](#)

 English (United States)

 Your Privacy Choices

 Theme

[Previous Versions](#)

[Blog](#)

[Contribute](#)

[Privacy](#)

[Terms of Use](#)

[Trademarks](#)

© Microsoft 2024