Microsoft Exchange Server

LetsEncrypt-Zertifikat in OnPrem-Exchange Server nutzen

Automatische Erstellung und Aktualisierung von kostenlosen LetsEncrypt-Zertifikaten für selbst gehostete (OnPrem-) Exchange Server mittels WIN-ACME

Voraussetzung: NAT von Port 80 (wg. Validierung) und Port 443 zum Exchange-Server

externer Name der externen URL sowie autodiscover-Subdomain sollte intern wie extern auf den Exchange-Server auflösen

Überprüfung z.B. per PowerShell:

Resolve-DnsName outlook.domain.com

Resolve-DnsName autodiscover.domain.com

sollte auf die interne IP-Adresse des Servers zeigen

Resolve-DnsName autodiscover.domain.com -server 8.8.8.8

Resolve-DnsName outlook.domain.com -server 8.8.8.8

sollte auf die externe IP-Adresse des Servers zeigen

(oder unter cmd entsprechend nslookup nutzen)

Das Tool WIN-ACME ruft ein kostenloses Let'sEncrypt-Zertifikat ab, bindet dieses im IIS des Exchange-Server ein und bindet auch automatisch die entsprechenden Exchange-Dienste an dieses Zertifikat. Außerdem sorgt ein geplanter Task dafür, dass das Zertifikat regelmäßig neu erstellt wird.

Aus den untenstehenden Beispiel-Scripts müssen lediglich die URLs an die eigenen Adressen angepasst werden.

Quelle: https://www.frankysweb.de/en/certificate-from-lets-encrypt-and-exchange-server-2019/

© 2026 David Horst <david.horst@ice-edv.com> | 2026-11-02 23:04
URL: https://ice-base.com/index.php?action=faq&cat=2&id=87&artlang=de

Microsoft Exchange Server

Automate certificate

To request a certificate from Let's Encrypt, renew it if necessary and configure it automatically for Exchange Server, the WIN-ACME Client can be used. In addition to Exchange servers, WIN-ACME also supports a whole range of other software such as RD Gateway and SQL Server.

In order to issue and configure a certificate for the Exchange Server, the WIN-ACME client must first be unpacked on the Exchange Server, in this example to D:\win-acme:

The directory contains the file settings_default.json, which can now be opened with the editor. In the file you will find the setting "PrivateKeyExportable" under the heading "Store". This setting is set to "false" by default. So that you can export the certificate later, this setting is set to "true" and the file is saved

To request a certificate and configure it automatically for Exchange, you need to customize a command. **Attention:** Note the language of the operating system

If Exchange is running on an operating system in **German language** is installed, you can use the following command and swap the hostnames outlook.domian.de andautodiscover.domain.de accordingly (this is where the authorizations for administrators and the network service are configured):

```
1
```

```
wacs.exe --source manual --host
outlook.domian.de,autodiscover.domain.de
--certificatestore My --acl-fullcontrol "Network
Service,Administrators" --installation iis,script
--installationsiteid 1 --script
"./Scripts/ImportExchange.v2.ps1"
--scriptparameters "'{CertThumbprint}'
'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}'
'{CertFriendlyName}'"
```

If Exchange is running on an operating system in **English language** is installed, you can use the following command and exchange the hostnames outlook.domian.de andautodiscover.domain.de accordingly (the authorizations for administrators and the network service are configured here):

```
1
```

```
wacs.exe --source manual --host
outlook.domian.de,autodiscover.domain.de
--certificatestore My --acl-fullcontrol "network
service,administrators" --installation iis,script
--installationsiteid 1 --script
"./Scripts/ImportExchange.v2.ps1"
--scriptparameters "'{CertThumbprint}'
'IIS,SMTP,IMAP' 1 '{CacheFile}' '{CachePassword}'
'{CertFriendlyName}'"
```


© 2026 David Horst <david.horst@ice-edv.com> | 2026-11-02 23:04
URL: https://ice-base.com/index.php?action=faq&cat=2&id=87&artlang=de

If the command is executed, the terms of use must be agreed to at the first start and an e-mail address for notifications must be entered:

The rest now happens automatically. A scheduled task is automatically created for the renewal of the certificate, which takes care of the update:

The certificate has also already been bound to the Exchange Services and activated, so nothing needs to be done manually here.

Check certificate

Finally, you should check whether the certificate is configured correctly. Outlook must not return any certificate error messages, and internal and external access via browsers (including Outlook, of course) must also work without certificate error messages. If there are still error messages, the problem lies with 99% as an incorrectly configured host name in the Exchange configuration or with the certificate.

As mentioned, Let's Encrypt certificates are valid for 90 days, so it makes sense to make an entry in the calendar in 80 days and check whether the certificate has been exchanged and everything has worked without any problems.

Eindeutige ID: #1086
Verfasser: David Horst
Letzte Änderung: 2026-03-28 17:38

© 2026 David Horst <david.horst@ice-edv.com> | 2026-11-02 23:04
URL: https://ice-base.com/index.php?action=faq&cat=2&id=87&artlang=de