

<https://docs.microsoft.com/en-us/exchange/troubleshoot/email-delivery/relay-access-denied-smtp>

- check **mail flow** / connector
inbound +
outbound
- **check**
TLScertificatedomain + Ipadresses

if it is scoped through **certificate** open

digicert.com/help

- enter the value for the domain you found above
- check both the * **certificate** and **smarthost**
- **smarthost** / **physical** address of the server → find the **actual certificate**
- **TLScertificatedomain** needs to be correct not to fail the check -
- if the actual doesnt match the authentication against the requested
TLScertificatedomain - change it

also if it is outbound connector the restrictdomainstocertificate prohibits any other domains

- **if the certificate is smarthost.domain restrictdomainstocertificate needs to be FALSE**
- you can check the IP to see the certificate behind for server
- **in both cases**
-same IP **OR** certificate
- should be confirmed or updated to be **distinct** for each connectors
to not cause a mail loop (hop count exceeded)