

# Phase 4 – Get connected

Step 3 – Test network connection



# DMS Import



Onboarding mini guide for System-to-System users



# Step 3

## Testing network connection

The next step is to verify the network access. If you are using the same certificate that has been set-up for production on DMS Export or Transit, you can skip this step.

The verification depends on the server style and can be executed in various ways. Which method to use is determined by the availability of tools on the client setup. See the next slides for different options.

### AS4 Server details for PRODUCTION:

Hostname: secureftpgateway.skat.dk

Port: 6384

IP: 195.85.251.102



# Unix

This section describes ways to test the connectivity on Unix-style servers, using common connectivity testing tools.

## Method #1 – telnet

```
telnet <Hostname> 6384
```

```
brj@T470PW10BRJ:~$ telnet secureftpgatewaytest.skat.dk 6384
Trying 195.85.251.85...
Connected to secureftpgatewaytest.skat.dk.
```

## Method #2 – nmap

```
Nmap -p 6384 <Hostname>
```

```
brj@T470PW10BRJ:~$ nmap -p 6384 secureftpgatewaytest.skat.dk
Nmap scan report for secureftpgatewaytest.skat.dk (195.85.251.85)
Host is up (0.0088s latency).

PORT      STATE SERVICE
6384/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.86 seconds
```

## Method #3 – openssl

```
openssl s_client -connect <Hostname>:443 -showcerts
```

```
brj@T470PW10BRJ:~$ openssl s_client -connect secureftpgatewaytest.skat.dk:443 -showcerts
CONNECTED(00000003)
depth=2 OU = GlobalSign Root CA - R3, O = GlobalSign, CN = GlobalSign
verify return:1
depth=1 C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
verify return:1
depth=0 C = DK, ST = Copenhagen, L = Copenhagen Oe, O = Skatteforvaltningen, CN = secureftpgatewaytest.skat.dk
verify return:1
139743226499712:error:14094410:SSL routines:ssl3_read_bytes:ssl3 alert handshake failure:../ssl/record/rec_layer_s3.c:1543:SSL alert number 40
---
Certificate chain
 0 s:C = DK, ST = Copenhagen, L = Copenhagen Oe, O = Skatteforvaltningen, CN = secureftpgatewaytest.skat.dk
 1:C = BE, O = GlobalSign nv-sa, CN = GlobalSign RSA OV SSL CA 2018
-----BEGIN CERTIFICATE-----
MIIGGjCCBZKgAwIBAgIMdnhIIn5QQEDWYMGVMAOGCSqGSIb3DQEBCwUAMFACzA3
BgNVBAYTAkQlJFMRKwFwYDQKExBHBG91YVxtaWduIG52LXNhMSYwJAYDVQQDEx1H
Bg91YVxtaWduIFJ0S0B0V1BTU0wGQ0EgMjAxODAwFw0xOTExMTUwODIxMDhaFw0y
MjAxMDQxMDEwMDZaMHhBxCA3BgNVBAYTAkRMRHwEYDQKIEwD3B1bmhhZ2ZVU
MRWYwFAYDVQQHEw1Db3B1bmhhZ2ZVUeI0MRWwGgYDVQQKExNTa2F0dGVmb3J2YVx0
bm1uZ2VvMSUwLWYwYDQKExxzZWm1cmVmdH8nYXR1d2F5dGVzdC5a2F0LmRrMTIIB
EjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA5x0n1pLz65JN9VAP1P3D2jK9
4gSB/FYPVvCs51fReb6KRqQA8N47LXqeIz9+q6vqh4+WAhgzqU5Q0b7TfYsI8R
0ep1f8CTb3UG/c3ypbz+x0DQF2y2jst0Q60v0L2GNpctfu0/HCF9Zwk1AxKdke7w
+8hwyZamao3w0wddq5JF0QkSU8rdoqgx+zJb1+o1cFqgazh1h8n2ge10FRZryG1
pP1SEUT/YZT2Q0wSDtqUTrFhAzhfPa5f1H2P1Rp3Yhg3KTk6BPAKRgrM5tT90uD
hags6mG7iCRTc1K2q7aExYwPwxyR8QcQ7ySM551AFU03o4c9e0651QFzWhzKSsID
AQAB04IDUzCCA08w0gYDVR0PAQH/BAQDAgWgMIGOBggrBgEFBQcBAQ5BgTB/MEQG
LCsGAQUFBzAChjh0dHRwO18vc2VjdXJlLmdsb2JhbHlpZ24uY29tL2NhY2VydC9n
E3JzYW92c3NsY2EynMDE4LmlydDA3BggrBgEFBQcwaYVYraHR0cDovL29jc3AuZ2xv
YmFsc21nb15jb20vZ3Nyc2FvdnNzbnBhbmhMjAxODAwBgNVHSAETzBNMEGCSsGAQOB
D0IBF0A8MDEGCCsGAQUFBwIBF1ZodHRwczovL3d3dy5nbG91YVxtaWduLmNvbnV5S9y
ZXBvc210b3J3L2A1BgZnGwBAGIwCQYDVRR0TBAIwADA/BgNVHR8EODAA2MD5gMqAw
h15odHRwO18vY3J3Lmdsb2JhbHlpZ24uY29tL2d3cnNhb3Zzc2x1YTIwMTguY3J3s
-----END CERTIFICATE-----
```

Phase 1

Send application form

Phase 2

Get the right roles and rights for TFE via Customer Portal

Register certificate on Certificate Portal TEST

Testing network connection DMS

Phase 3

Develop/integration DMS

Test with clients

Phase 4

DMS Production

Onboarding process view

# Windows

This section describes ways to test the connectivity on Windows-style servers using common connectivity testing tools.

This method requires execution in Powershell.

```
Test-NetConnection <Hostname>-Port 6384
```

```
PS Z:\> Test-NetConnection secureftpgatewaytest.skat.dk -Port 6384

ComputerName      : secureftpgatewaytest.skat.dk
RemoteAddress     : 195.85.251.85
RemotePort        : 6384
InterfaceAlias    : Ethernet 67
SourceAddress     : 192.168.146.12
TcpTestSucceeded  : True
```

# General test

Open <https://<Hostname>:6384> in a browser that has access to the internet - on a client setup that the internal network is set up as the accessing system. If it works, you will receive a 404 error.





# Appendix

Please turn to the extended [Connectivity guide](#) if you need more information about the AS4 Gateway. Furthermore, we recommend to visit the [AS4 Simple Client package](#) made for facilitating a client which can communicate with the AS4 portal and through it, the DMS Import system.

It covers the following:

- Converting an XML format declaration to an AS4 message
- Handles connectivity to the AS4 gateway
- Encryption and signing of AS4 messages
- Sending AS4 messages to AS4 gateway
- Receiving replies from AS4 gateway

The package is written in Java and provided as Java dependency. Integration with .NET based projects is therefore not as simple. For .NET based projects we recommend building a small Java based communication middleman REST API, which utilizes the simple AS4 client, that the existing .NET code can communicate with.

Need technical support?

Go to [Customer Portal \(Toolkit\)](#) to book an online session or ask your question. To see frequently asked questions: Go to the website above click Documents and download **DMS Onboarding – FAQ**.