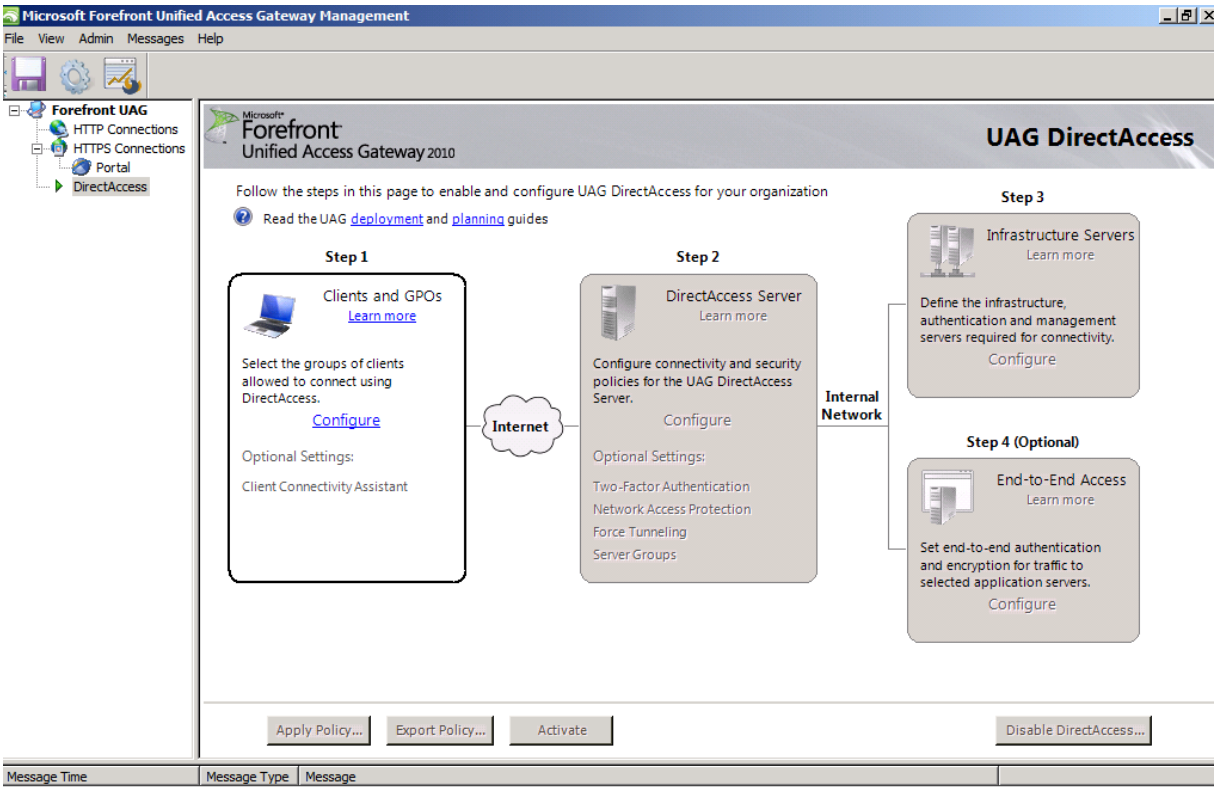
Forefront UAG DirectAccess mit SP1 Release Candidate (RC)

Dieses Bilderbuch beschreibt nur die Aenderungen in Forefront UAG SP1 RC.

Details zu UAG und UAG DA:
http://www.it-training-grote.de/download/FF-UAG-DA.pdf
http://www.it-training-grote.de/download/FF-UAG-nrw2010.pdf
http://www.it-training-grote.de/download/Forefront-UAG.pdf
http://www.it-training-grote.de/download/UAG-Array.pdf
http://www.it-training-grote.de/download/UAG-DA-T-mobile.pdf
http://www.it-training-grote.de/download/UAG-DA-Vodafone.pdf
http://www.it-training-grote.de/download/UAG-DA.pdf
http://www.it-training-grote.de/download/UAG-Update1.pdf
http://www.it-training-grote.de/download/UAG.pdf
http://www.it-training-grote.de/download/UAG2010Beta.pdf

Assistent starten



Clients and GPOs Configuration

Clients and GPOs Configuration

- Deployment Model
- Client Domains
- Policy Management
- Client Groups

You can deploy Forefront UAG DirectAccess to connect DirectAccess clients to internal networks, and for remote management of DirectAccess clients.

(•) Allow DirectAccess clients to connect to internal networks, and enable remote management of DirectAccess clients

( ) Enable remote management of DirectAccess clients only

[ ] Allow only services running under the client computer account to access infrastructure servers used for remote management

When you allow clients to access the internal network, you can configure settings that include client authentication, NAP Enforcement and forced tunneling. If you select remote client management only, these features are not available.

Learn more... | < Back | Next > | Finish | Cancel

Clients and GPOs Configuration

Clients and GPOs Configuration

- Deployment Model
- Client Domains
- Policy Management
- Client Groups

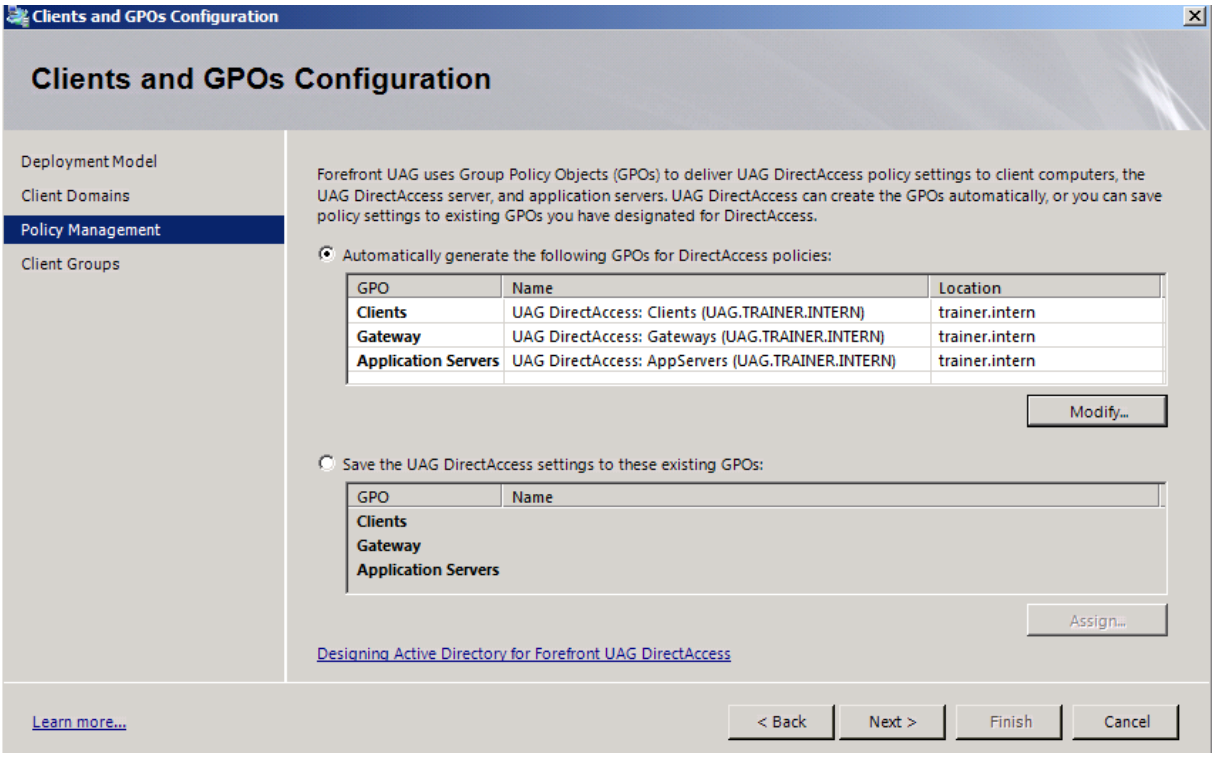
Specify the domains in which the client computers allowed to connect using Forefront UAG DirectAccess reside. Policy settings contained in the UAG DirectAccess clients Group Policy object (GPO) will be applied to these computers.

Enable DirectAccess for client computers in these domains:

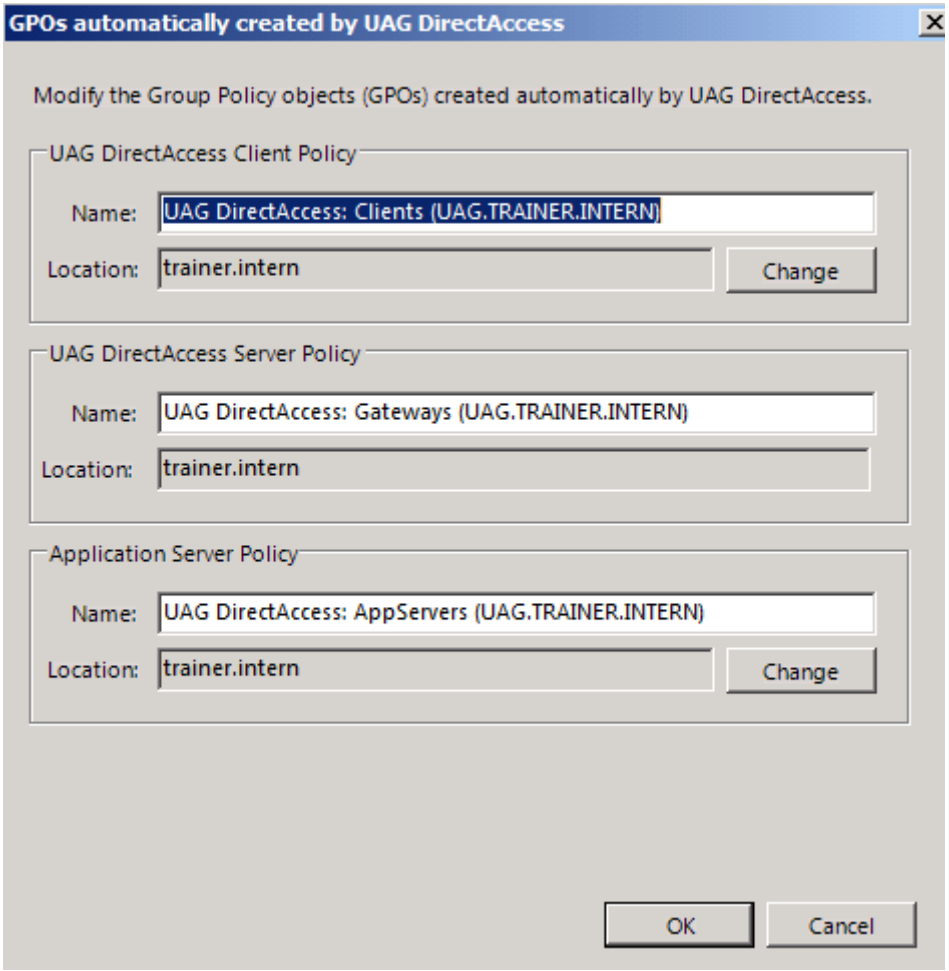
trainer.intern

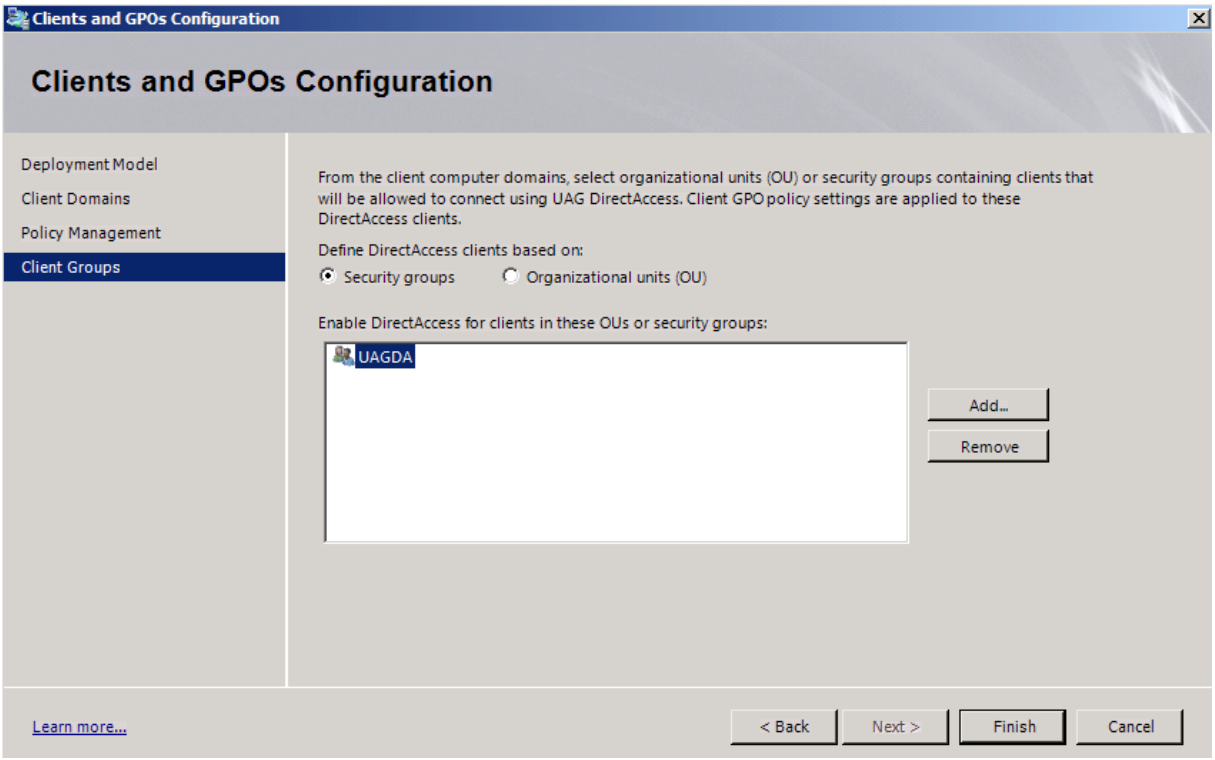
Add... | Remove

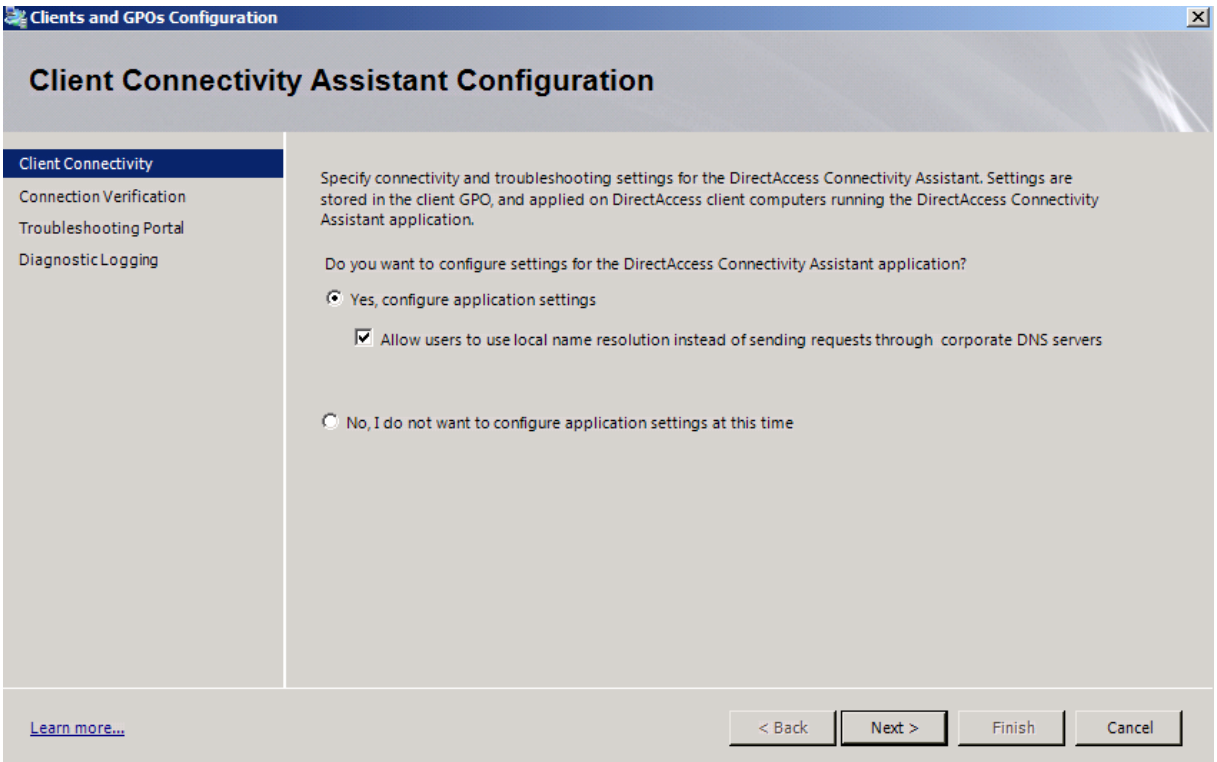
Learn more... | < Back | Next > | Finish | Cancel

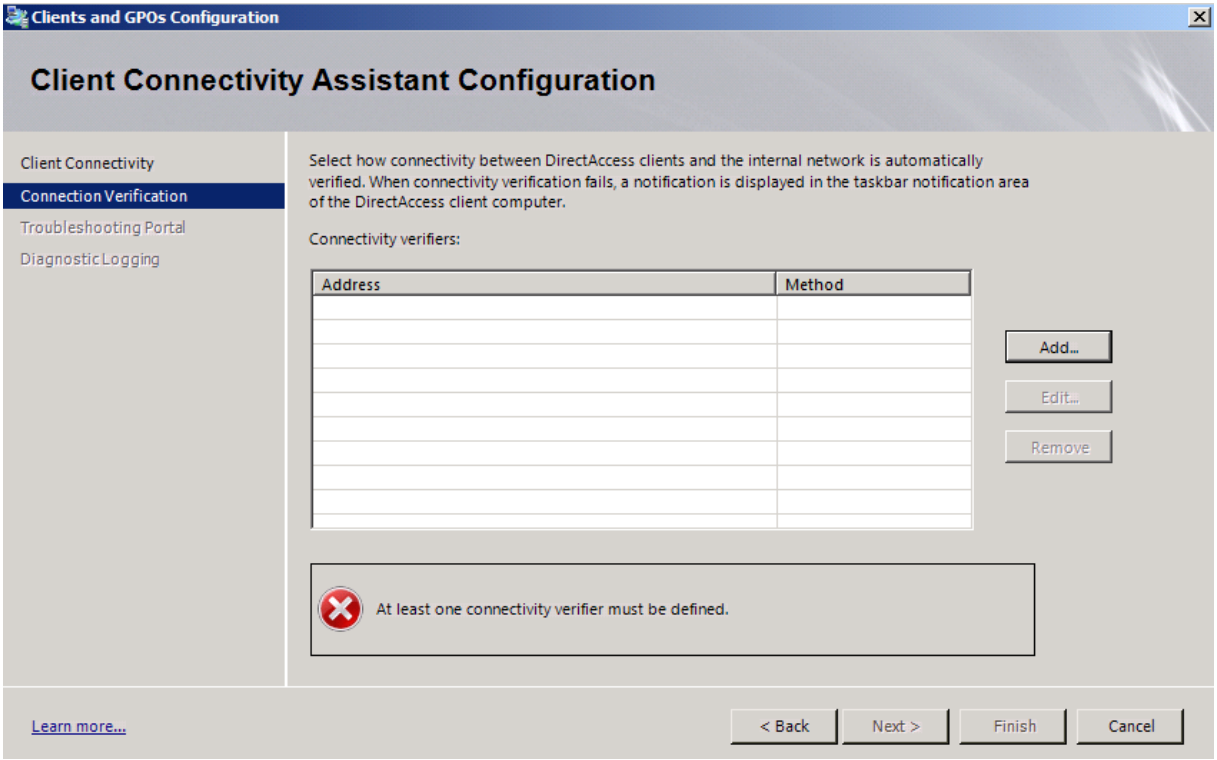


GPO modifizieren (optional)

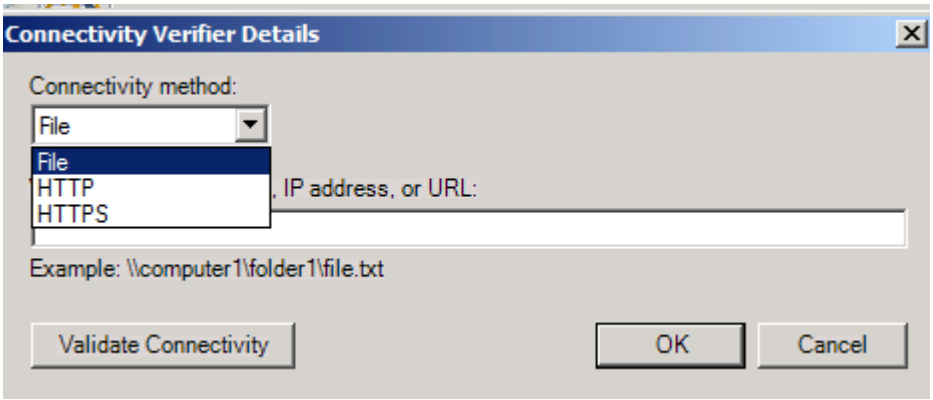


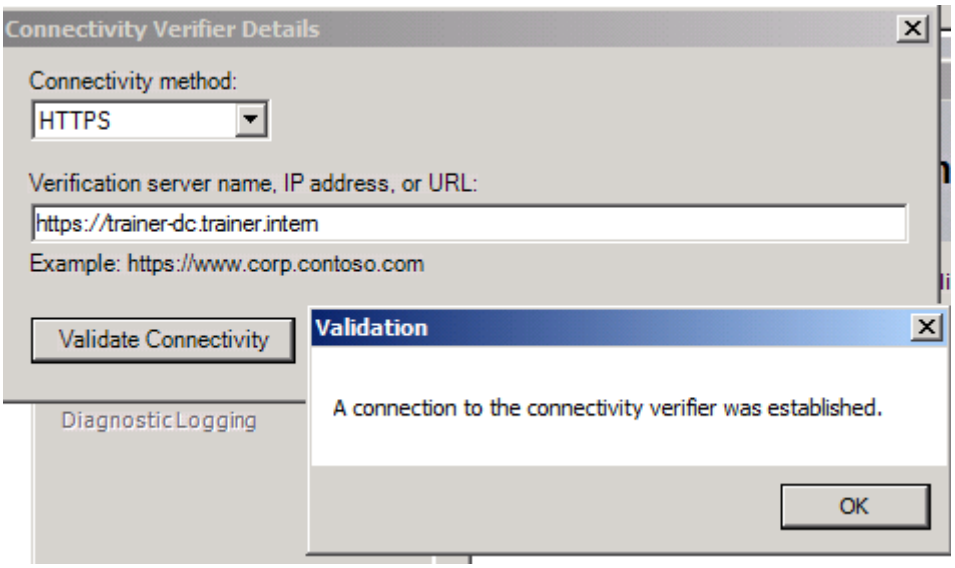

Clients and GPOs Configuration
Clients and GPOs Configuration
Deployment Model
Client Domains
Policy Management
Client Groups
From the client computer domains, select organizational units (OU) or security groups containing clients that will be allowed to connect using UAG DirectAccess. Client GPO policy settings are applied to these DirectAccess clients.
Define DirectAccess clients based on:
Security groups
Organizational units (OU)
Enable DirectAccess for clients in these OUs or security groups:
UAGDA
Add...
Remove
Learn more...
< Back
Next >
Finish
Cancel


Clients and GPOs Configuration
Client Connectivity Assistant Configuration
Client Connectivity
Connection Verification
Troubleshooting Portal
Diagnostic Logging
Specify connectivity and troubleshooting settings for the DirectAccess Connectivity Assistant. Settings are stored in the client GPO, and applied on DirectAccess client computers running the DirectAccess Connectivity Assistant application.
Do you want to configure settings for the DirectAccess Connectivity Assistant application?
Yes, configure application settings
Allow users to use local name resolution instead of sending requests through corporate DNS servers
No, I do not want to configure application settings at this time
Learn more...
< Back
Next >
Finish
Cancel

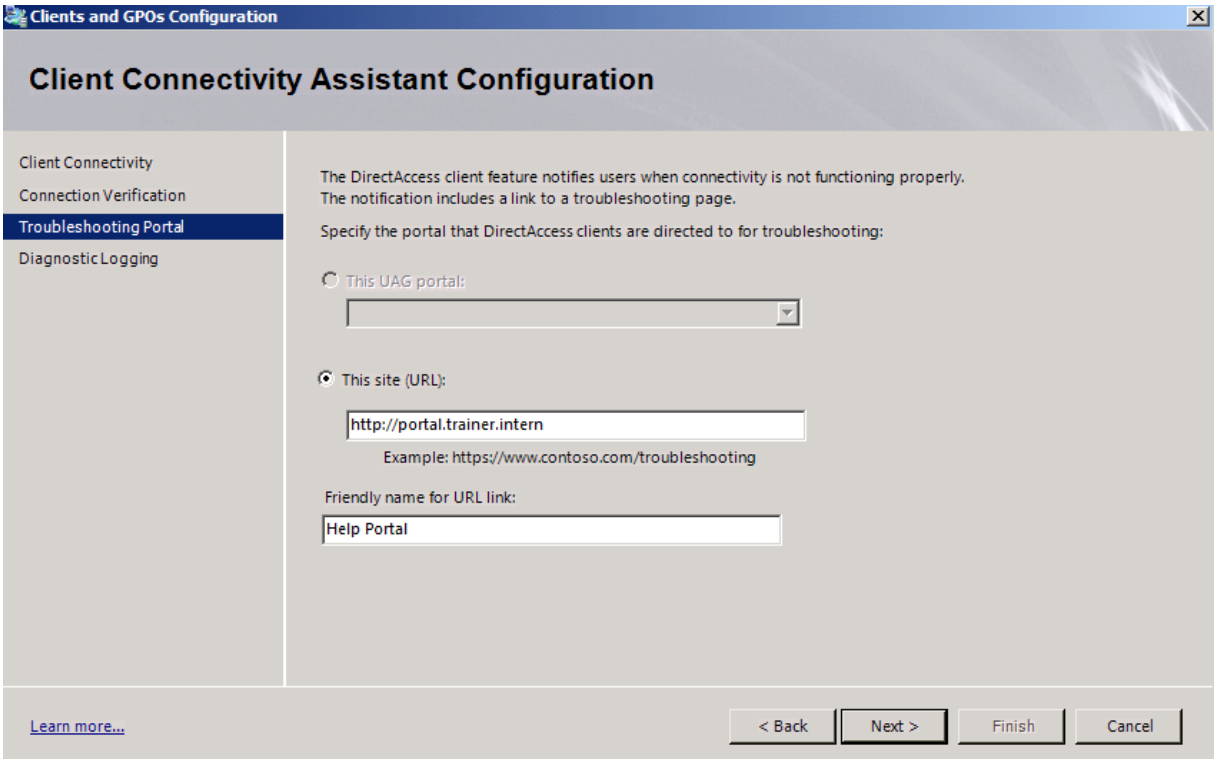

Clients and GPOs Configuration
Client Connectivity Assistant Configuration
Client Connectivity
Connection Verification
Troubleshooting Portal
Diagnostic Logging
Select how connectivity between DirectAccess clients and the internal network is automatically verified. When connectivity verification fails, a notification is displayed in the taskbar notification area of the DirectAccess client computer.
Connectivity verifiers:
Address
Method
Add...
Edit...
Remove
At least one connectivity verifier must be defined.
Learn more...
< Back
Next >
Finish
Cancel

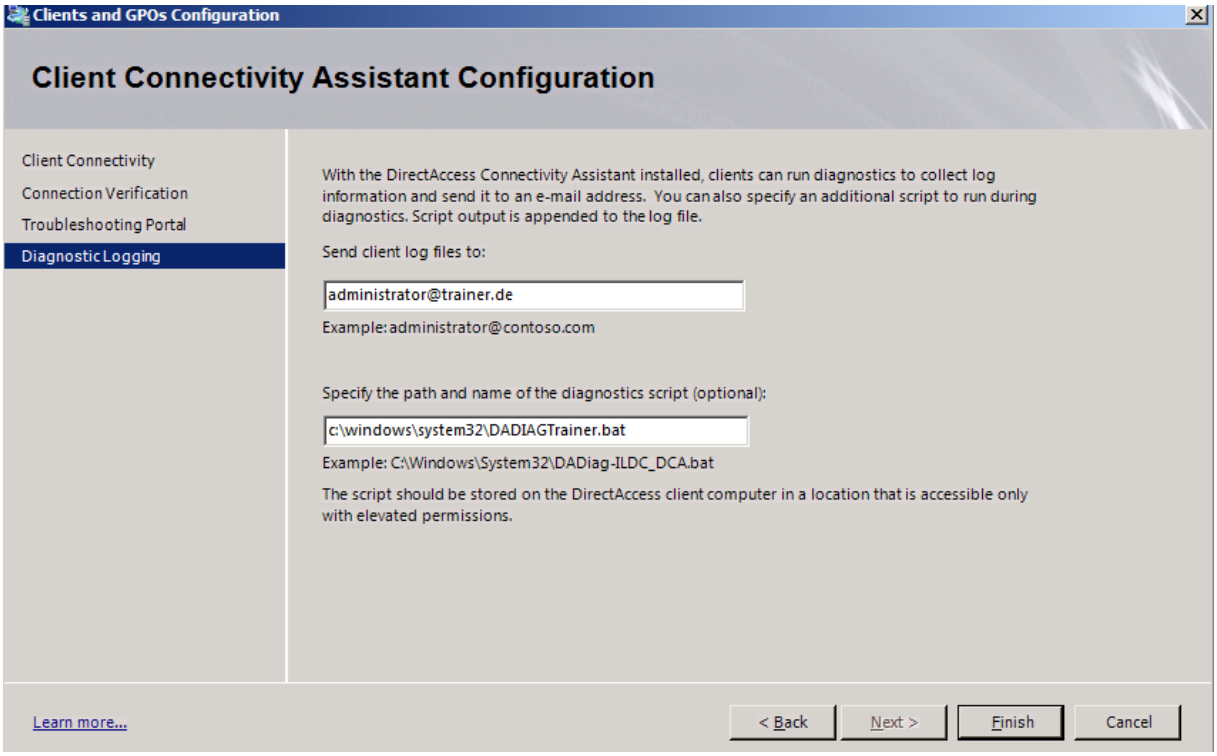
Neu und cool!

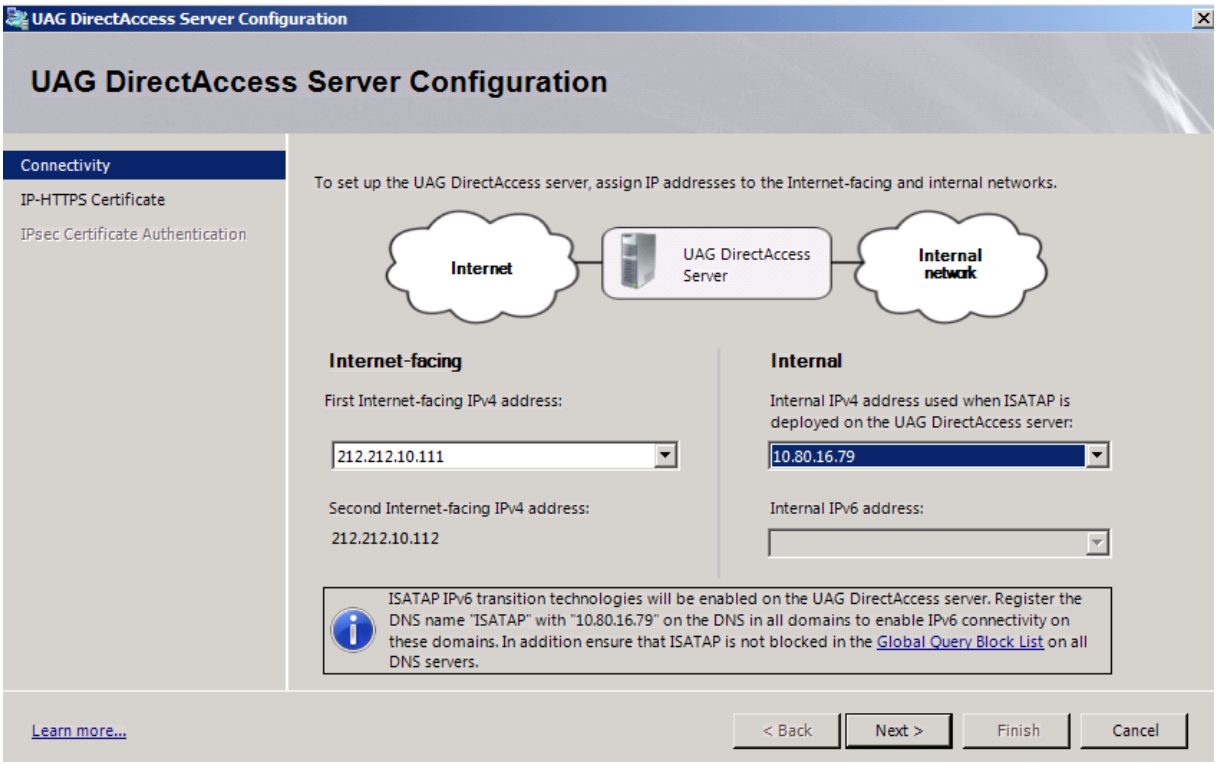

Connectivity Verifier Details
Connectivity method:
File
File
HTTP
HTTPS
, IP address, or URL:
Example: \\computer1\folder1\file.txt
Validate Connectivity
OK
Cancel

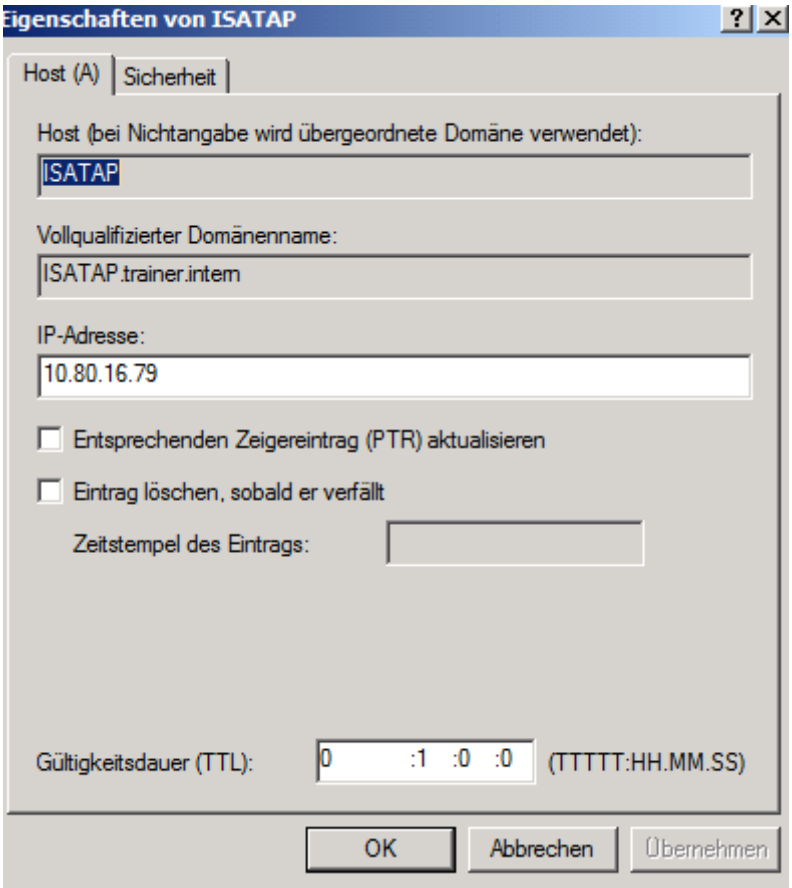

Connectivity Verifier Details
Connectivity method:
HTTPS
Verification server name, IP address, or URL:
https://trainer-dc.trainer.intern
Example: https://www.corp.contoso.com
Validate Connectivity
Diagnostic Logging
Validation
A connection to the connectivity verifier was established.
OK

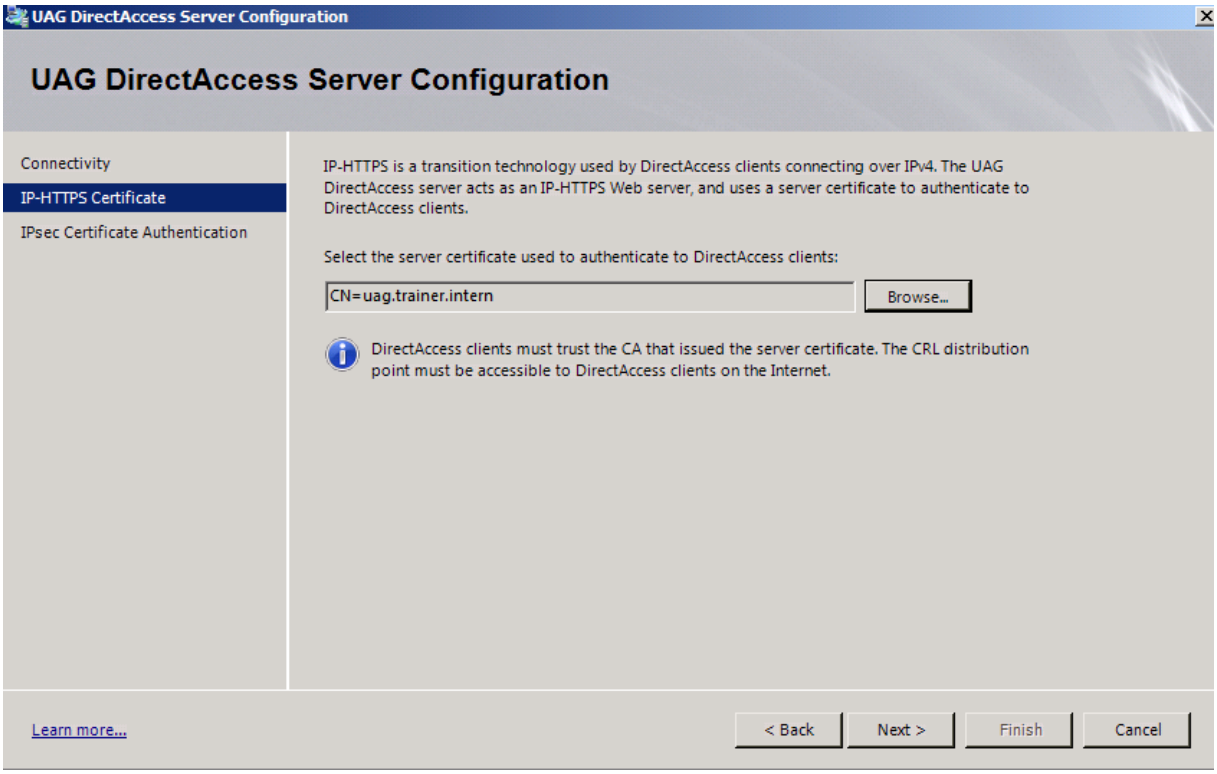
Version 1.5 des Connectivity Assistenten ist verfuegbar (bisher 1.0) und auch nicht ueber den Assistenten konfigurierbar

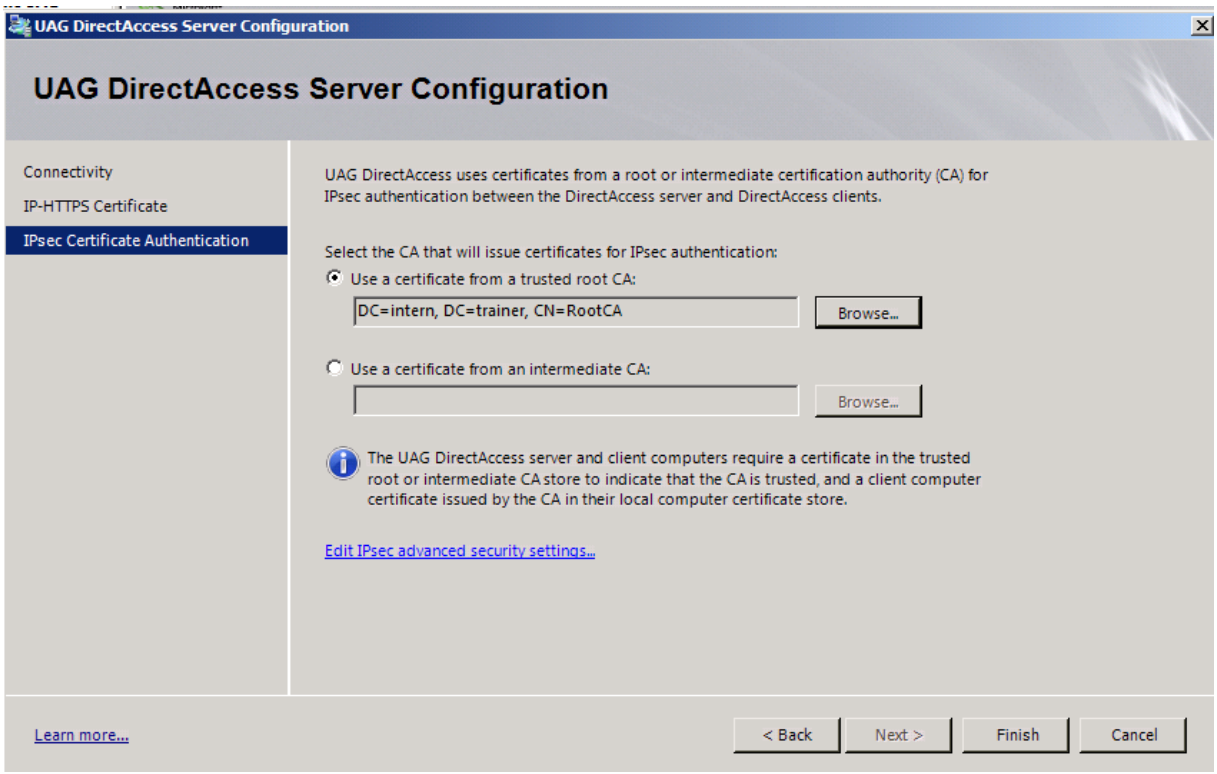




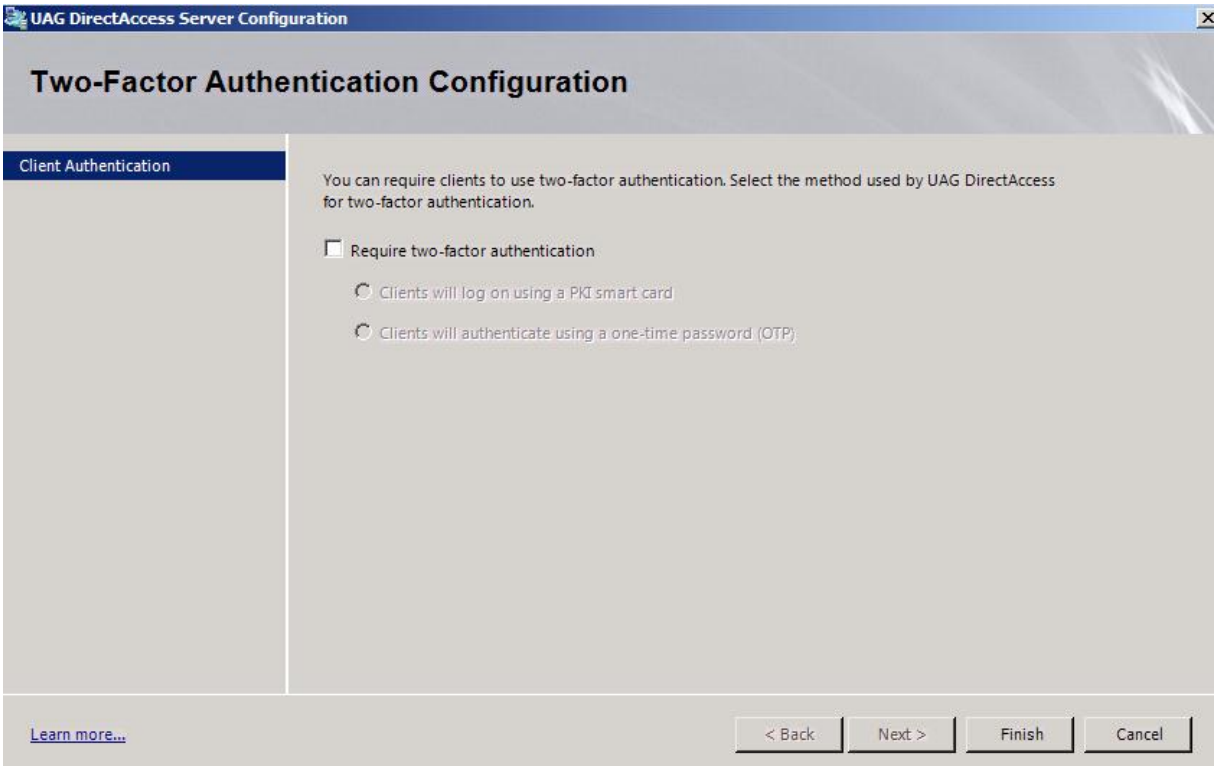

UAG DirectAccess Server Configuration
UAG DirectAccess Server Configuration
Connectivity
IP-HTTPS Certificate
IPsec Certificate Authentication
To set up the UAG DirectAccess server, assign IP addresses to the Internet-facing and internal networks.
Internet
UAG DirectAccess Server
Internal network
Internet-facing
First Internet-facing IPv4 address:
212.212.10.111
Second Internet-facing IPv4 address:
212.212.10.112
Internal
Internal IPv4 address used when ISATAP is deployed on the UAG DirectAccess server:
10.80.16.79
Internal IPv6 address:
ISATAP IPv6 transition technologies will be enabled on the UAG DirectAccess server. Register the DNS name "ISATAP" with "10.80.16.79" on the DNS in all domains to enable IPv6 connectivity on these domains. In addition ensure that ISATAP is not blocked in the Global Query Block List on all DNS servers.
Learn more...
< Back
Next >
Finish
Cancel

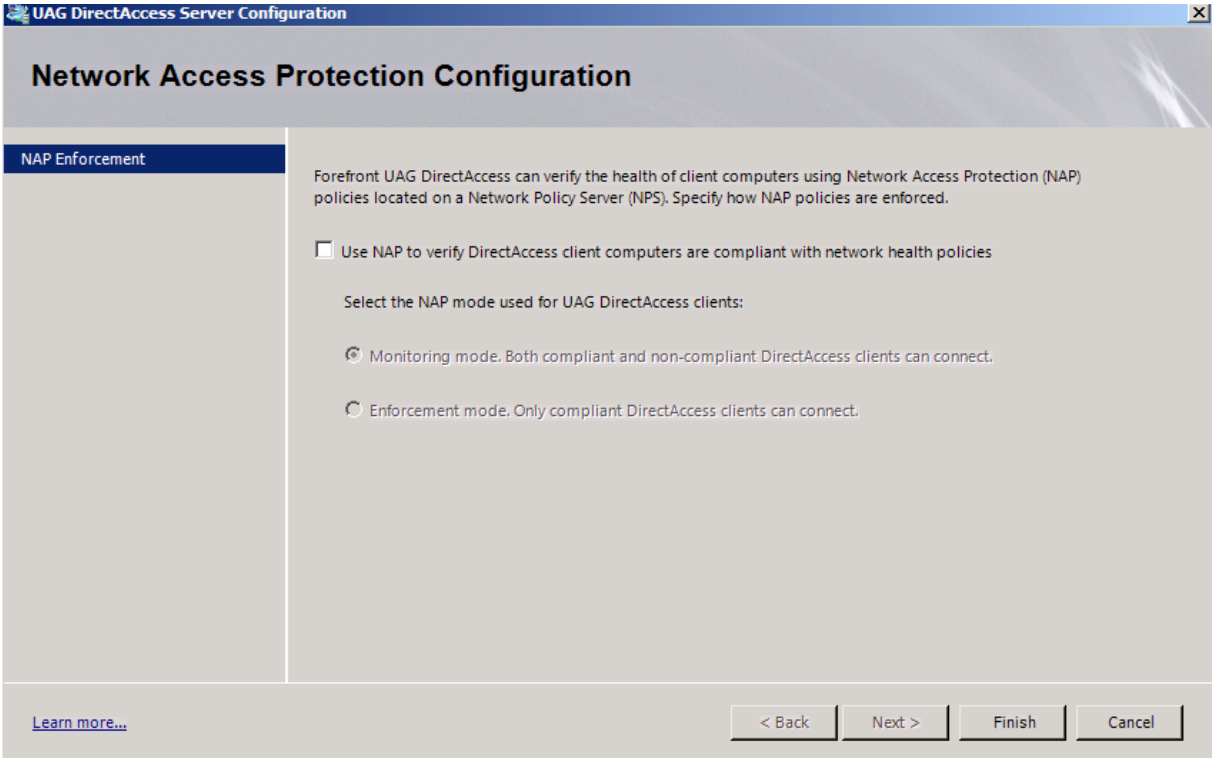

Eigenschaften von ISATAP
Host (A)
Sicherheit
Host (bei Nichtangabe wird übergeordnete Domäne verwendet):
ISATAP
Vollqualifizierter Domänenname:
ISATAP.trainer.intern
IP-Adresse:
10.80.16.79
Entsprechenden Zeigereintrag (PTR) aktualisieren
Eintrag löschen, sobald er verfällt
Zeitstempel des Eintrags:
Gültigkeitsdauer (TTL):
0 :1 :0 :0
(TTTTT:HH.MM.SS)
OK
Abbrechen
Übernehmen


UAG DirectAccess Server Configuration
UAG DirectAccess Server Configuration
Connectivity
IP-HTTPS Certificate
IPsec Certificate Authentication
IP-HTTPS is a transition technology used by DirectAccess clients connecting over IPv4. The UAG DirectAccess server acts as an IP-HTTPS Web server, and uses a server certificate to authenticate to DirectAccess clients.
Select the server certificate used to authenticate to DirectAccess clients:
CN=uag.trainer.intern
Browse...
DirectAccess clients must trust the CA that issued the server certificate. The CRL distribution point must be accessible to DirectAccess clients on the Internet.
Learn more...
< Back
Next >
Finish
Cancel

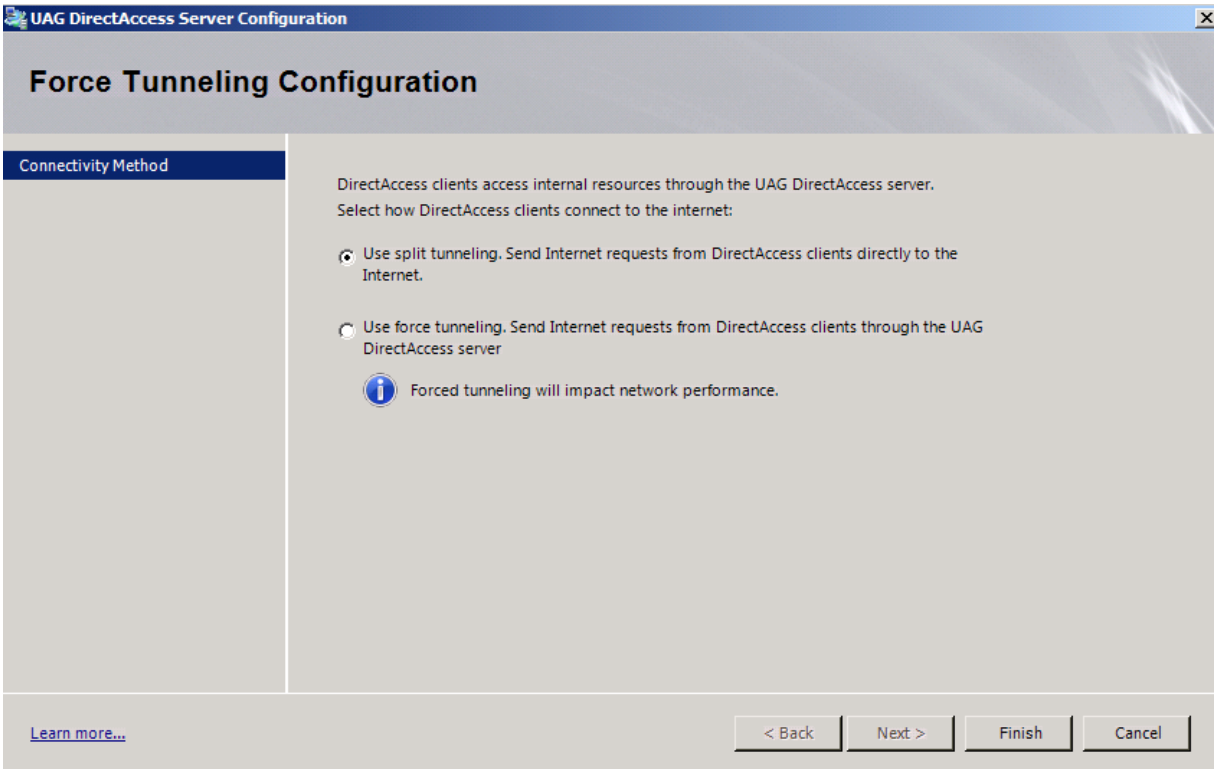

UAG DirectAccess Server Configuration
UAG DirectAccess Server Configuration
Connectivity
IP-HTTPS Certificate
IPsec Certificate Authentication
UAG DirectAccess uses certificates from a root or intermediate certification authority (CA) for IPsec authentication between the DirectAccess server and DirectAccess clients.
Select the CA that will issue certificates for IPsec authentication:
Use a certificate from a trusted root CA:
DC=intern, DC=trainer, CN=RootCA
Browse...
Use a certificate from an intermediate CA:
Browse...
The UAG DirectAccess server and client computers require a certificate in the trusted root or intermediate CA store to indicate that the CA is trusted, and a client computer certificate issued by the CA in their local computer certificate store.
Edit IPsec advanced security settings...
Learn more...
< Back
Next >
Finish
Cancel

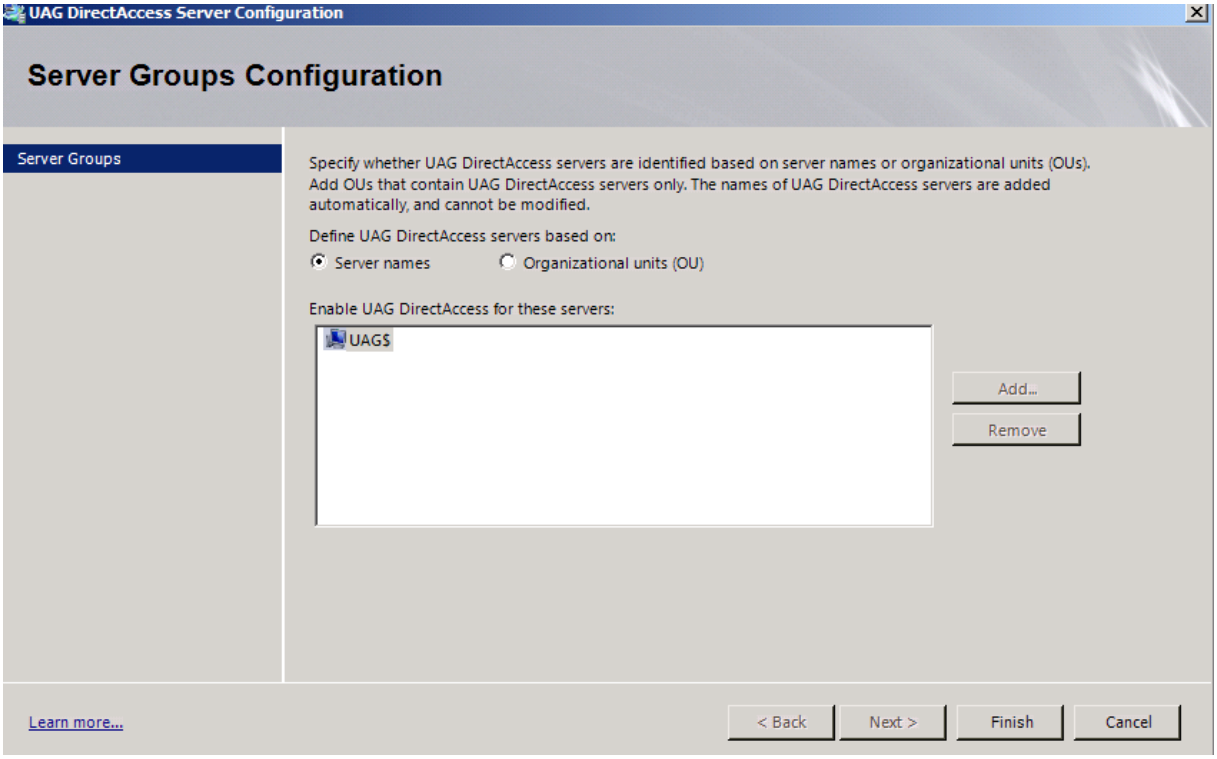
Optional

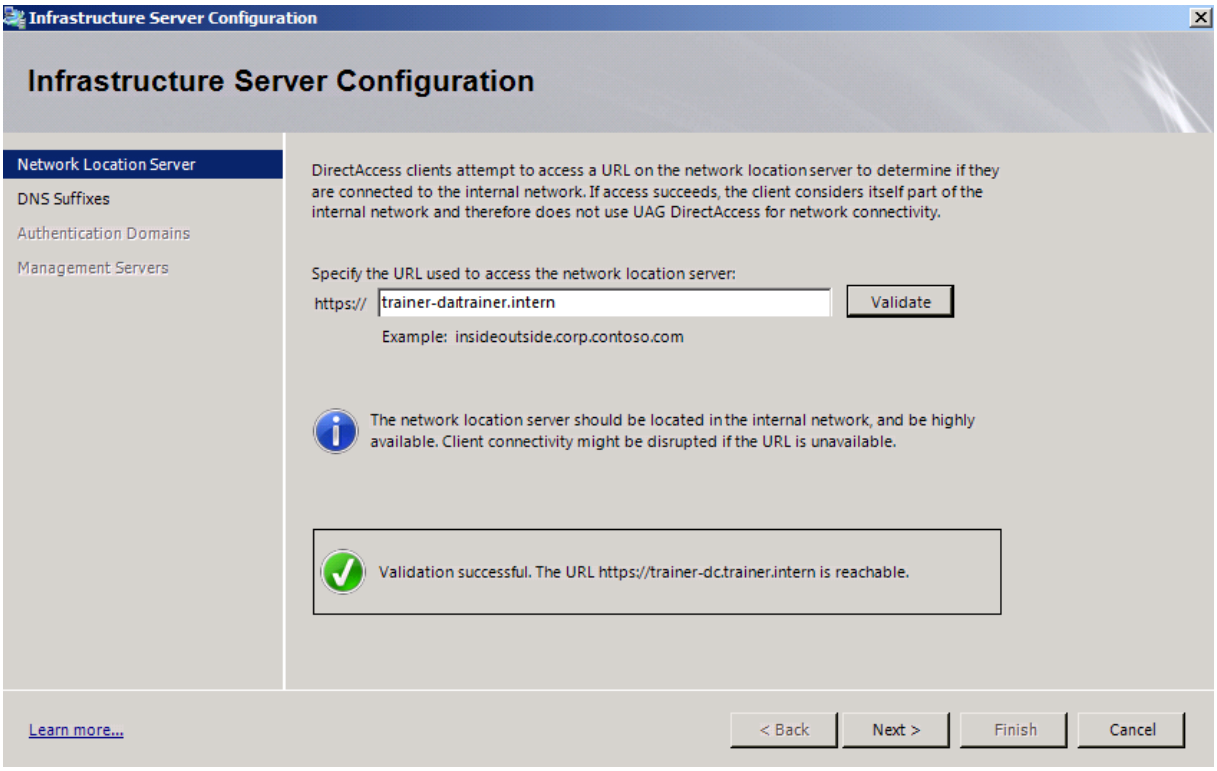

UAG DirectAccess Server Configuration
Two-Factor Authentication Configuration
Client Authentication
You can require clients to use two-factor authentication. Select the method used by UAG DirectAccess for two-factor authentication.
Require two-factor authentication
Clients will log on using a PKI smart card
Clients will authenticate using a one-time password (OTP)
Learn more...
< Back
Next >
Finish
Cancel

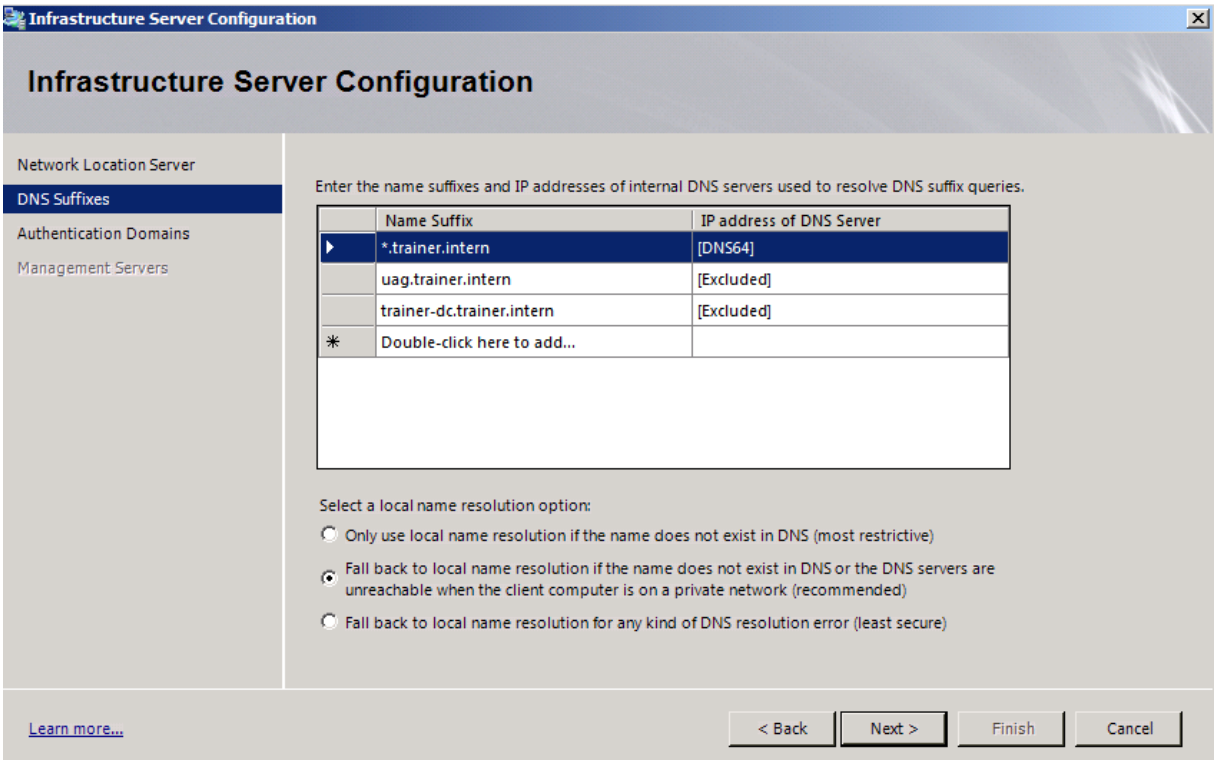

UAG DirectAccess Server Configuration
Network Access Protection Configuration
NAP Enforcement
Forefront UAG DirectAccess can verify the health of client computers using Network Access Protection (NAP) policies located on a Network Policy Server (NPS). Specify how NAP policies are enforced.
Use NAP to verify DirectAccess client computers are compliant with network health policies
Select the NAP mode used for UAG DirectAccess clients:
Monitoring mode. Both compliant and non-compliant DirectAccess clients can connect.
Enforcement mode. Only compliant DirectAccess clients can connect.
Learn more...
< Back
Next >
Finish
Cancel

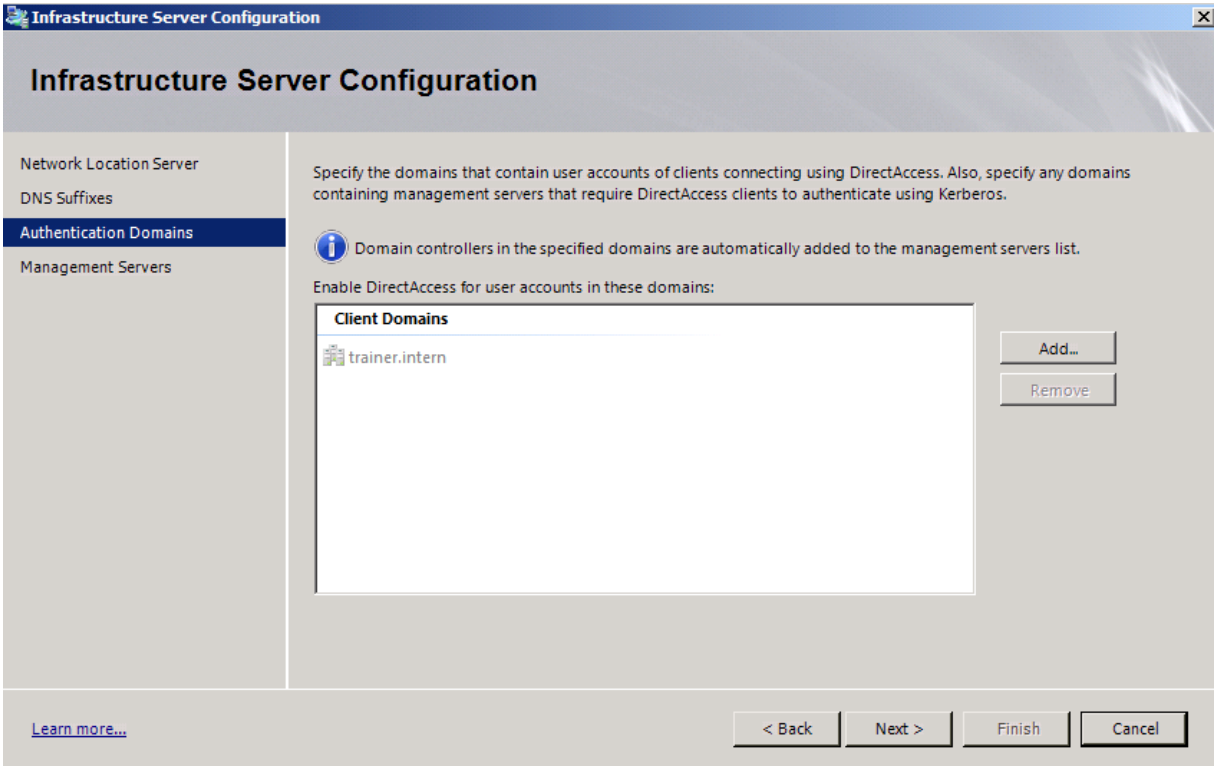
Endlich

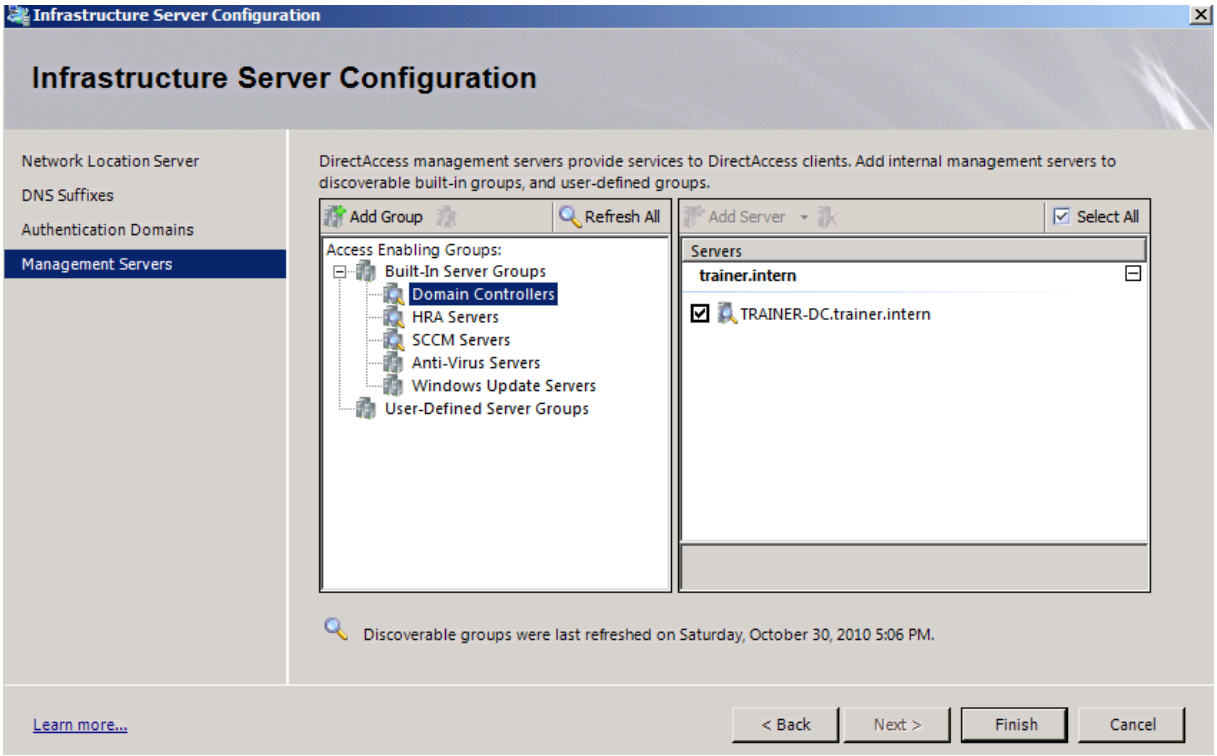

UAG DirectAccess Server Configuration
Force Tunneling Configuration
Connectivity Method
DirectAccess clients access internal resources through the UAG DirectAccess server.
Select how DirectAccess clients connect to the internet:
Use split tunneling. Send Internet requests from DirectAccess clients directly to the Internet.
Use force tunneling. Send Internet requests from DirectAccess clients through the UAG DirectAccess server
Forced tunneling will impact network performance.
Learn more...
< Back
Next >
Finish
Cancel


UAG DirectAccess Server Configuration
Server Groups Configuration
Server Groups
Specify whether UAG DirectAccess servers are identified based on server names or organizational units (OUs). Add OUs that contain UAG DirectAccess servers only. The names of UAG DirectAccess servers are added automatically, and cannot be modified.
Define UAG DirectAccess servers based on:
Server names
Organizational units (OU)
Enable UAG DirectAccess for these servers:
UAG$
Add...
Remove
Learn more...
< Back
Next >
Finish
Cancel

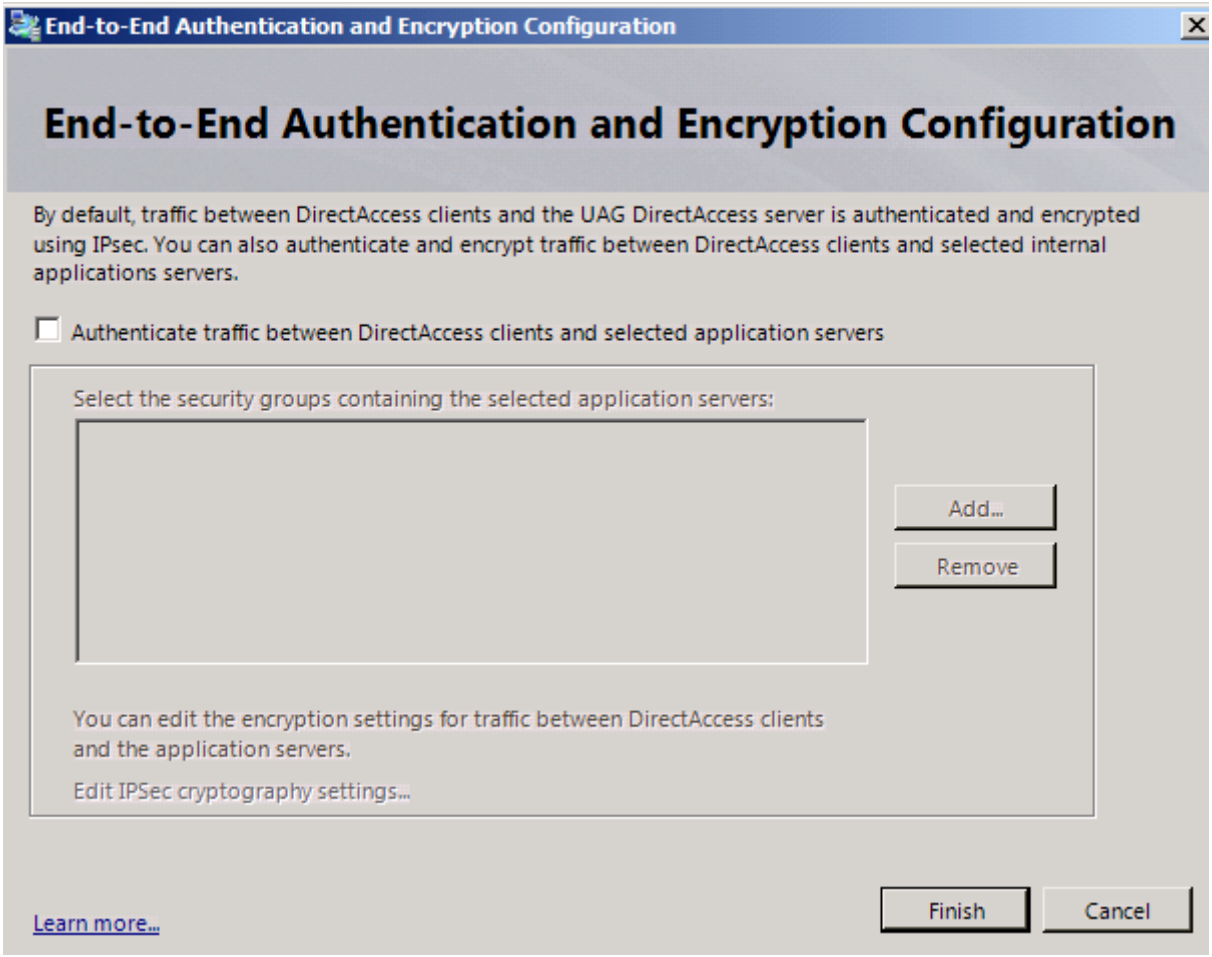

Infrastructure Server Configuration
Infrastructure Server Configuration
Network Location Server
DNS Suffixes
Authentication Domains
Management Servers
DirectAccess clients attempt to access a URL on the network location server to determine if they are connected to the internal network. If access succeeds, the client considers itself part of the internal network and therefore does not use UAG DirectAccess for network connectivity.
Specify the URL used to access the network location server:
https://
trainer-dc.trainer.intern
Validate
Example: insideoutside.corp.contoso.com
The network location server should be located in the internal network, and be highly available. Client connectivity might be disrupted if the URL is unavailable.
Validation successful. The URL https://trainer-dc.trainer.intern is reachable.
Learn more...
< Back
Next >
Finish
Cancel


Infrastructure Server Configuration
Infrastructure Server Configuration
Network Location Server
DNS Suffixes
Authentication Domains
Management Servers
Enter the name suffixes and IP addresses of internal DNS servers used to resolve DNS suffix queries.
Name Suffix
IP address of DNS Server
*.trainer.intern
[DNS64]
uag.trainer.intern
[Excluded]
trainer-dc.trainer.intern
[Excluded]
Double-click here to add...
Select a local name resolution option:
Only use local name resolution if the name does not exist in DNS (most restrictive)
Fall back to local name resolution if the name does not exist in DNS or the DNS servers are unreachable when the client computer is on a private network (recommended)
Fall back to local name resolution for any kind of DNS resolution error (least secure)
Learn more...
< Back
Next >
Finish
Cancel


Infrastructure Server Configuration
Infrastructure Server Configuration
Network Location Server
DNS Suffixes
Authentication Domains
Management Servers
Specify the domains that contain user accounts of clients connecting using DirectAccess. Also, specify any domains containing management servers that require DirectAccess clients to authenticate using Kerberos.
Domain controllers in the specified domains are automatically added to the management servers list.
Enable DirectAccess for user accounts in these domains:
Client Domains
trainer.intern
Add...
Remove
Learn more...
< Back
Next >
Finish
Cancel


Infrastructure Server Configuration
Infrastructure Server Configuration
Network Location Server
DNS Suffixes
Authentication Domains
Management Servers
DirectAccess management servers provide services to DirectAccess clients. Add internal management servers to discoverable built-in groups, and user-defined groups.
Add Group
Refresh All
Add Server
Select All
Access Enabling Groups:
Built-In Server Groups
Domain Controllers
HRA Servers
SCCM Servers
Anti-Virus Servers
Windows Update Servers
User-Defined Server Groups
Servers
trainer.intern
TRAINER-DC.trainer.intern
Discoverable groups were last refreshed on Saturday, October 30, 2010 5:06 PM.
Learn more...
< Back
Next >
Finish
Cancel

Optional


End-to-End Authentication and Encryption Configuration
End-to-End Authentication and Encryption Configuration
By default, traffic between DirectAccess clients and the UAG DirectAccess server is authenticated and encrypted using IPsec. You can also authenticate and encrypt traffic between DirectAccess clients and selected internal applications servers.
Authenticate traffic between DirectAccess clients and selected application servers
Select the security groups containing the selected application servers:
Add...
Remove
You can edit the encryption settings for traffic between DirectAccess clients and the application servers.
Edit IPSec cryptography settings...
Learn more...
Finish
Cancel

Forefront UAG DirectAccess Configuration Review

Forefront UAG DirectAccess Configuration Review

Group policy objects were generated with these settings. If the settings are correct, click"Apply Now" to apply the policies.

DirectAccess Client Settings

- Apply GPO client policies to these security groups:

  UAGDA

- Apply deployment mode:
  - Allow access to internal networks, and remote management
- DirectAccess Connectivity Assistant settings:
  - Verify connectivity using:
    - HTTP:https://trainer-dc.trainer.intern
  - Allow local name resolution: enabled.
  - Troubleshooting site: http://portal.trainer.intern
  - Troubleshooting help link: Help Portal
  - Send log file to email: administrator@trainer.de
  - Optional script location: c:\windows\system32\DADIAGTrainer.bat

DirectAccess Server Settings

- DirectAccess server Internet-facing address: "*212.212.10.111*"

Learn more...

Apply Now | Print Review | Cancel

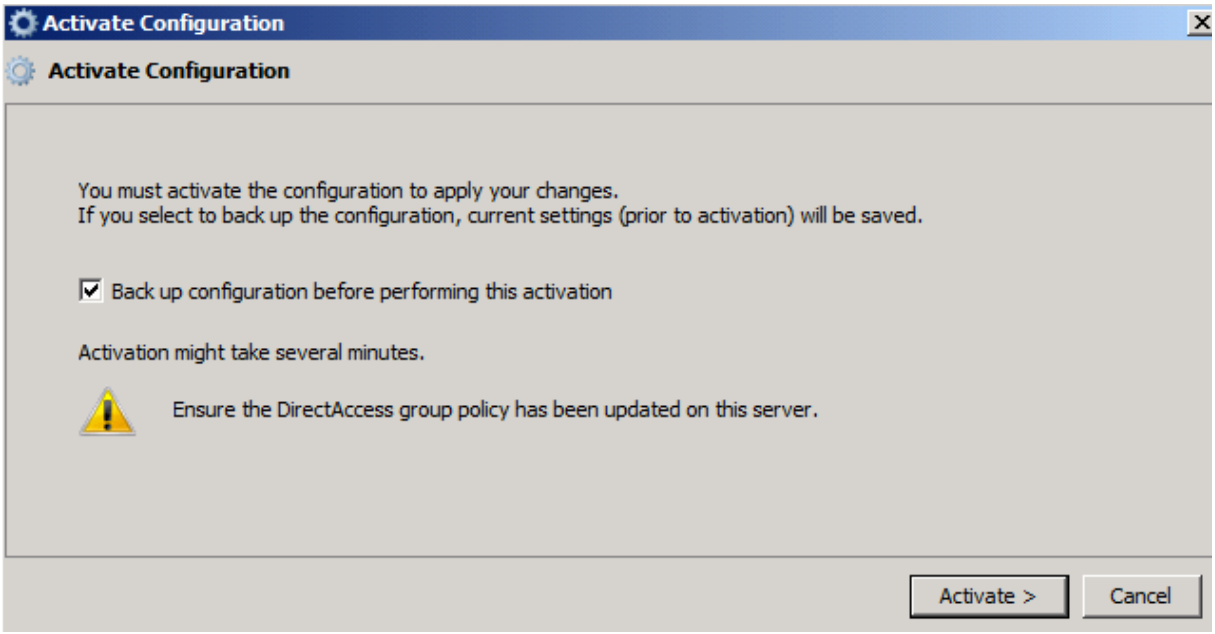
DirectAccess Policy Configuration

Policy Configuration Log:

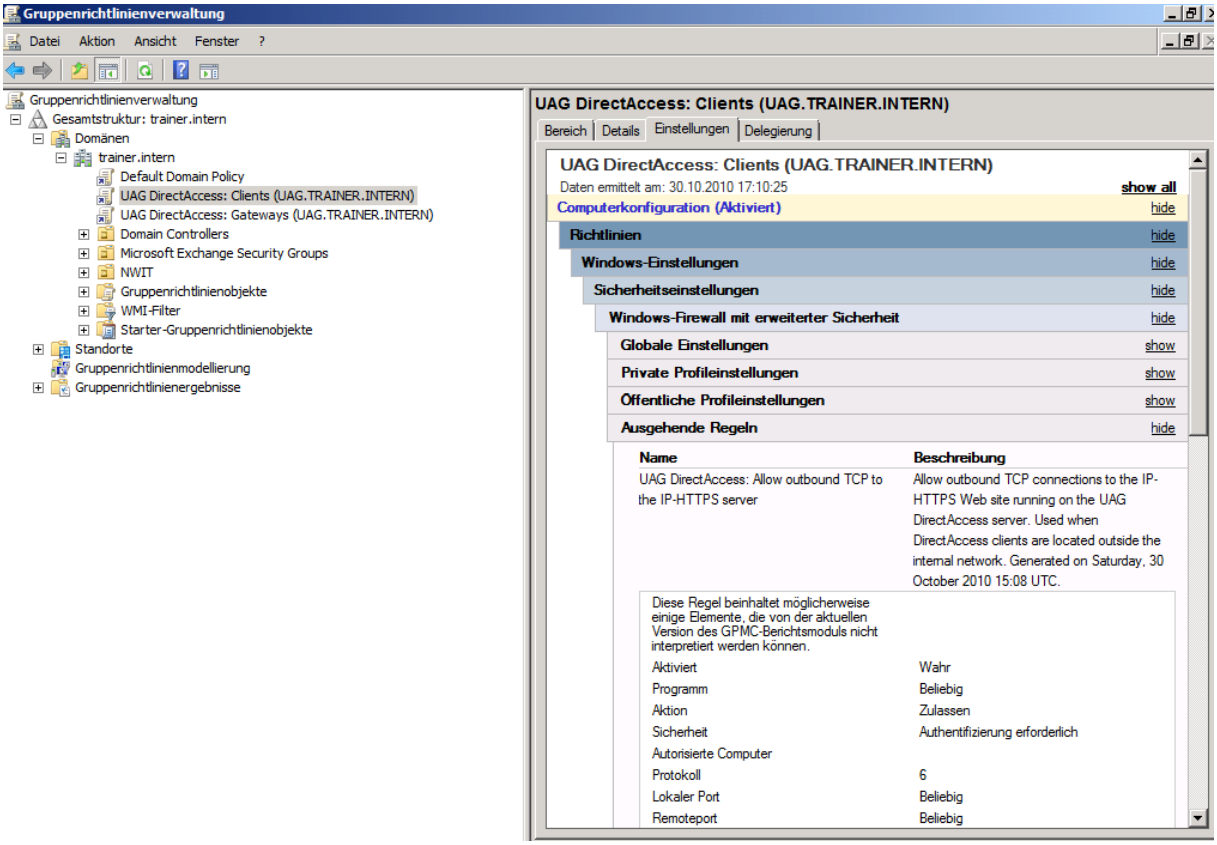
```
> Clearing all links for GPO 'UAG DirectAccess: AppServers (UAG.TRAINER
  > Done!
Clearing all links for GPO 'UAG DirectAccess: AppServers (UAG.TRAINER.I
Checking if GPO 'UAG DirectAccess: AppServers (UAG.TRAINER.INTERN)' in
> Trying to find GPO 'UAG DirectAccess: AppServers (UAG.TRAINER.INTERN)
  GPO 'UAG DirectAccess: AppServers (UAG.TRAINER.INTERN)' found
> Checking if the GPO 'UAG DirectAccess: AppServers (UAG.TRAINER.INTERN
  The GPO is writable
>> Configuring trainer.intern\UAG DirectAccess: AppServers (UAG.TRAINER
Executing Reset local GPO for trainer.intern\UAG DirectAccess: AppServe
done.
Executing Export local policy to file ...
done.
Executing Import from export-file to domain gpo=trainer.intern\UAG Dire
done.

============ UAGDA Group Policy Apply Completed. Elapsed time is 00:00:

 Script run completed with no errors or warnings.
```

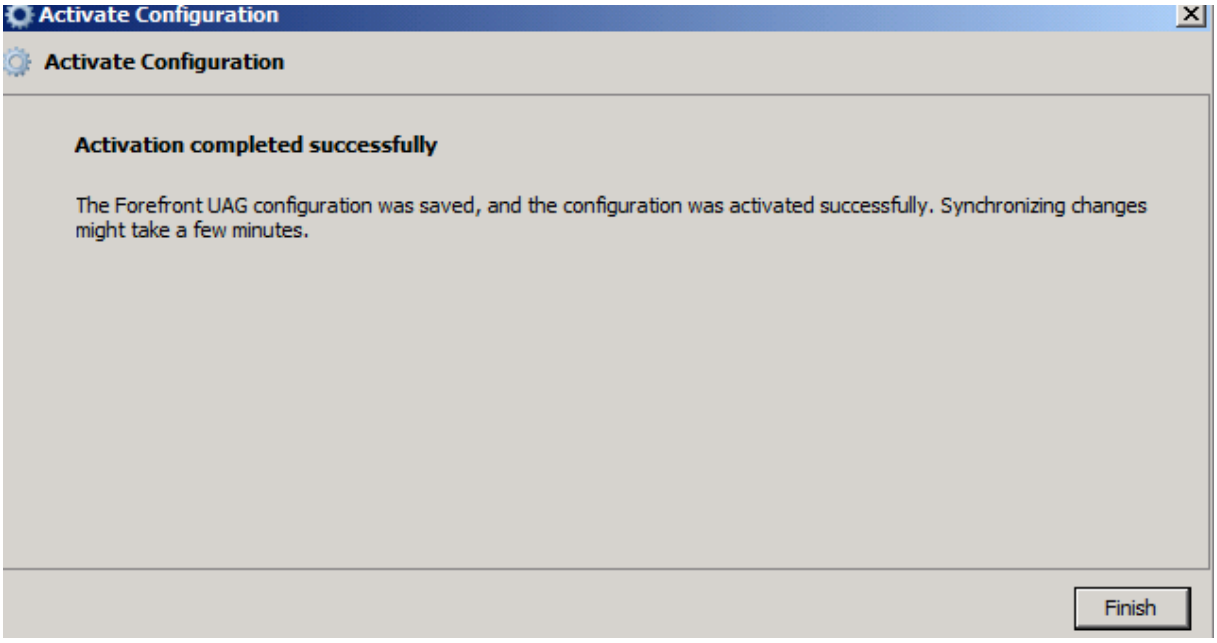
OK | Cancel

Save config and activate (dauert jetzt auch nicht mehr ganz so lange)

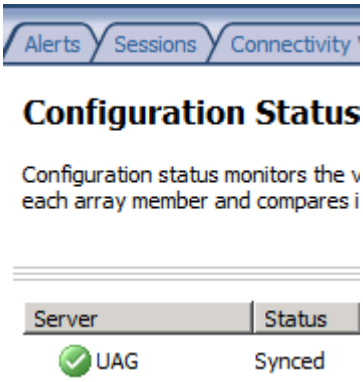


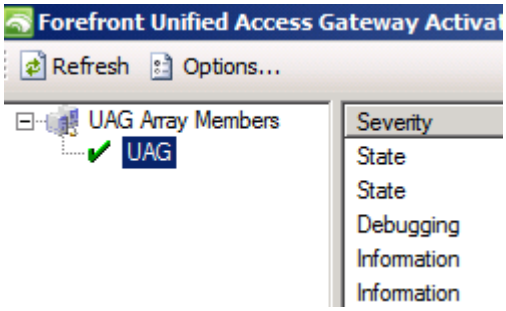
Erstellte Gruppenrichtlinien





Sync abwarten





Nach dem naechsten Update der Gruppenrichtlinienverarbeitung auf den Windows 7 Clients ist UAG DA verfuegbar!

Have fun