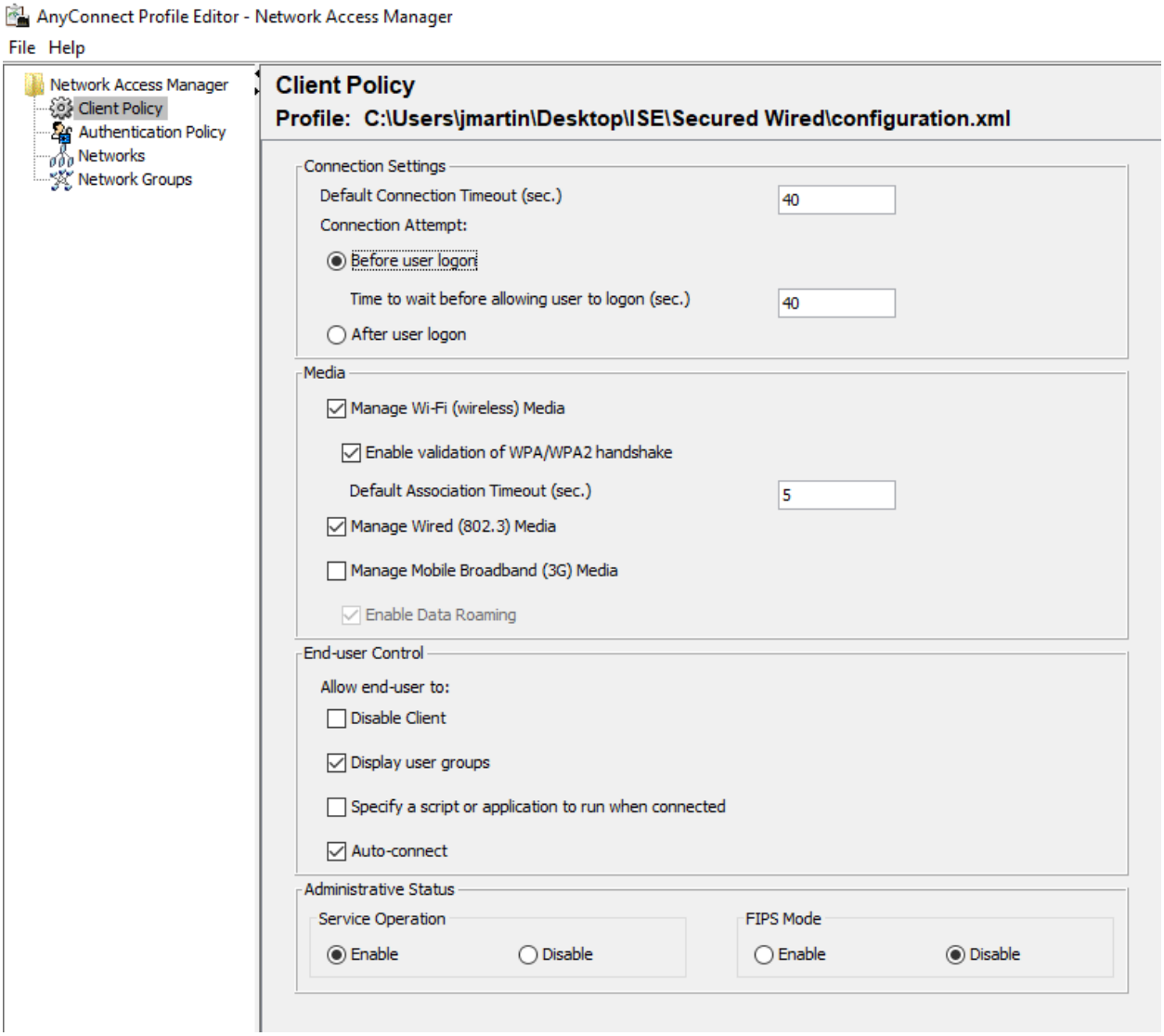
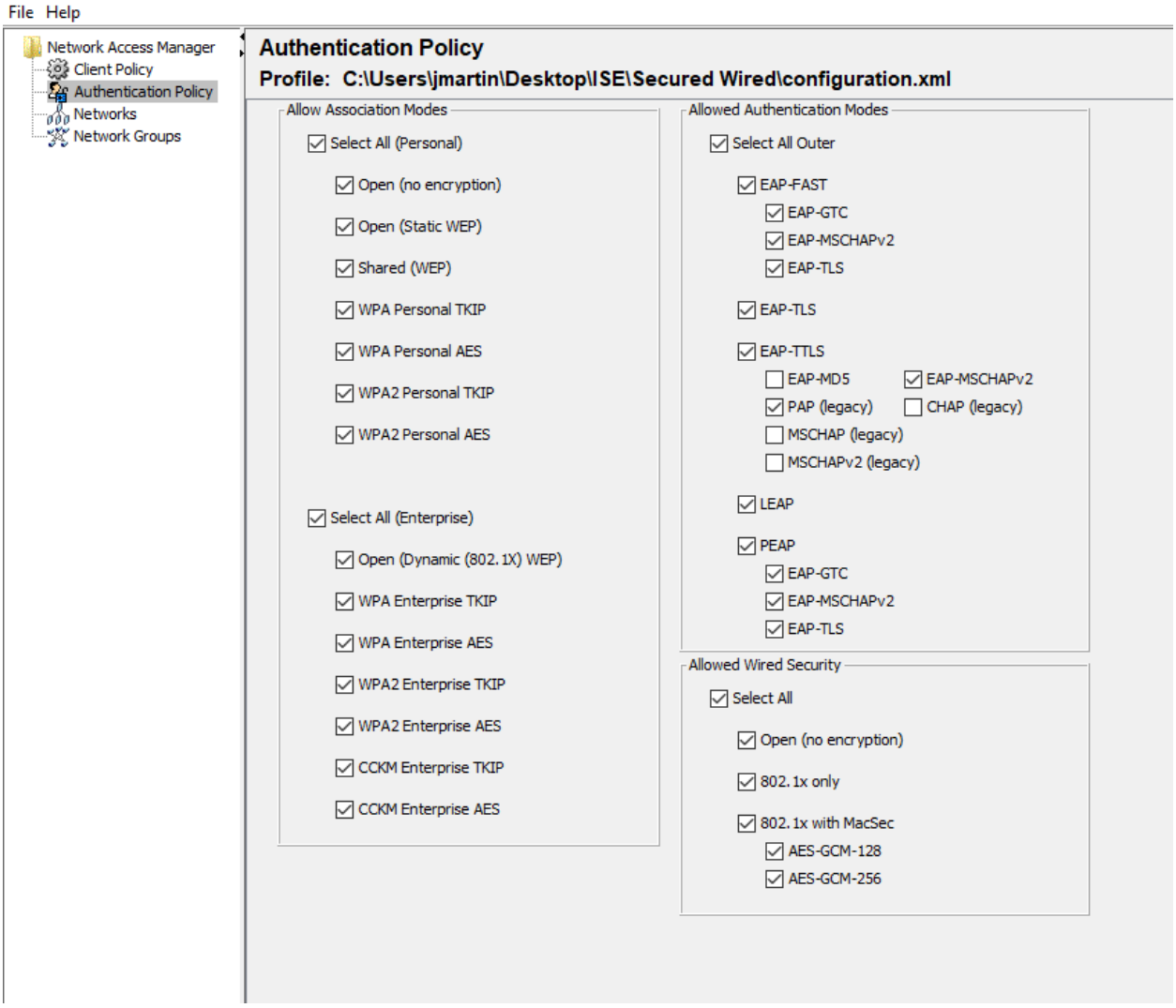
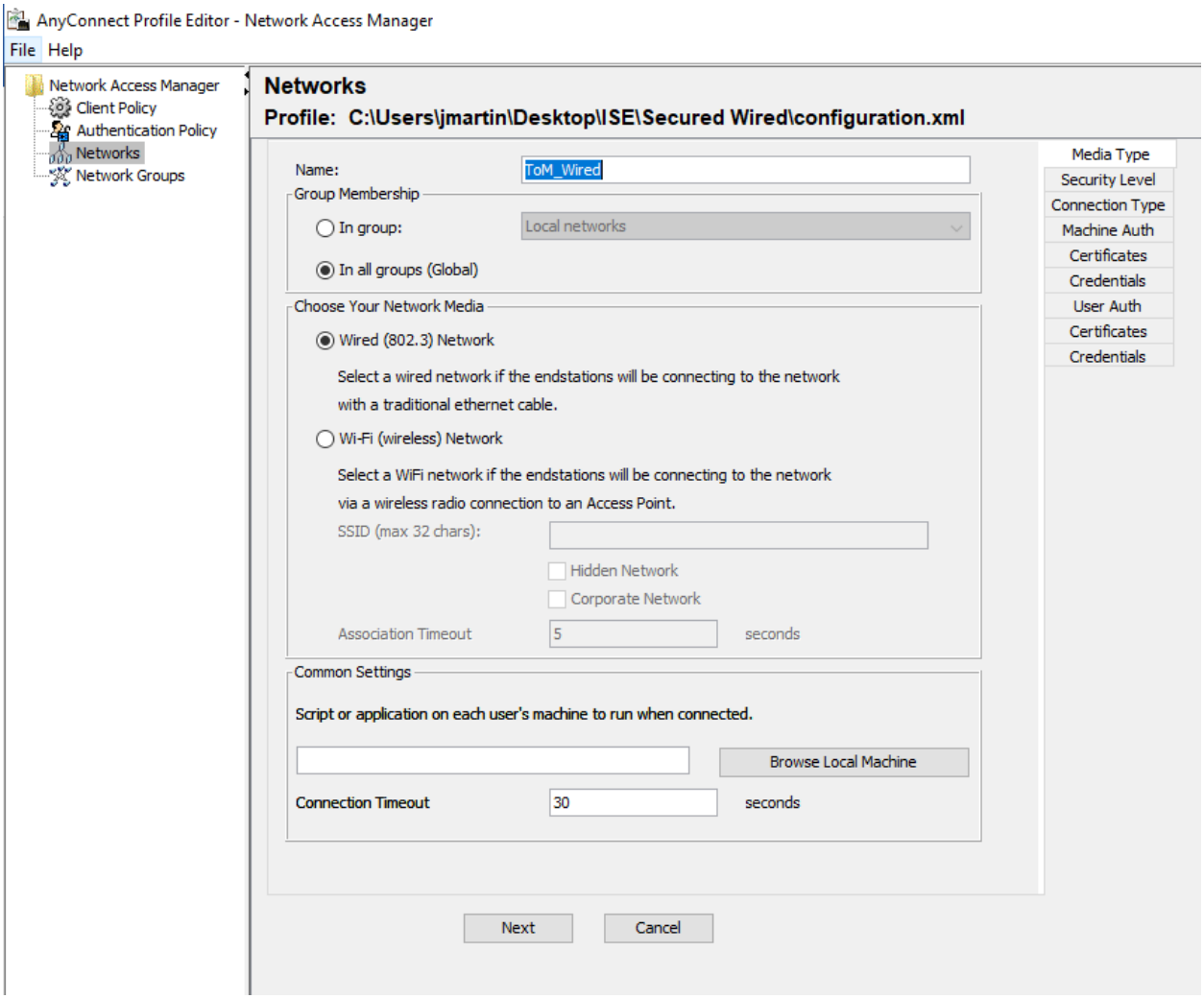
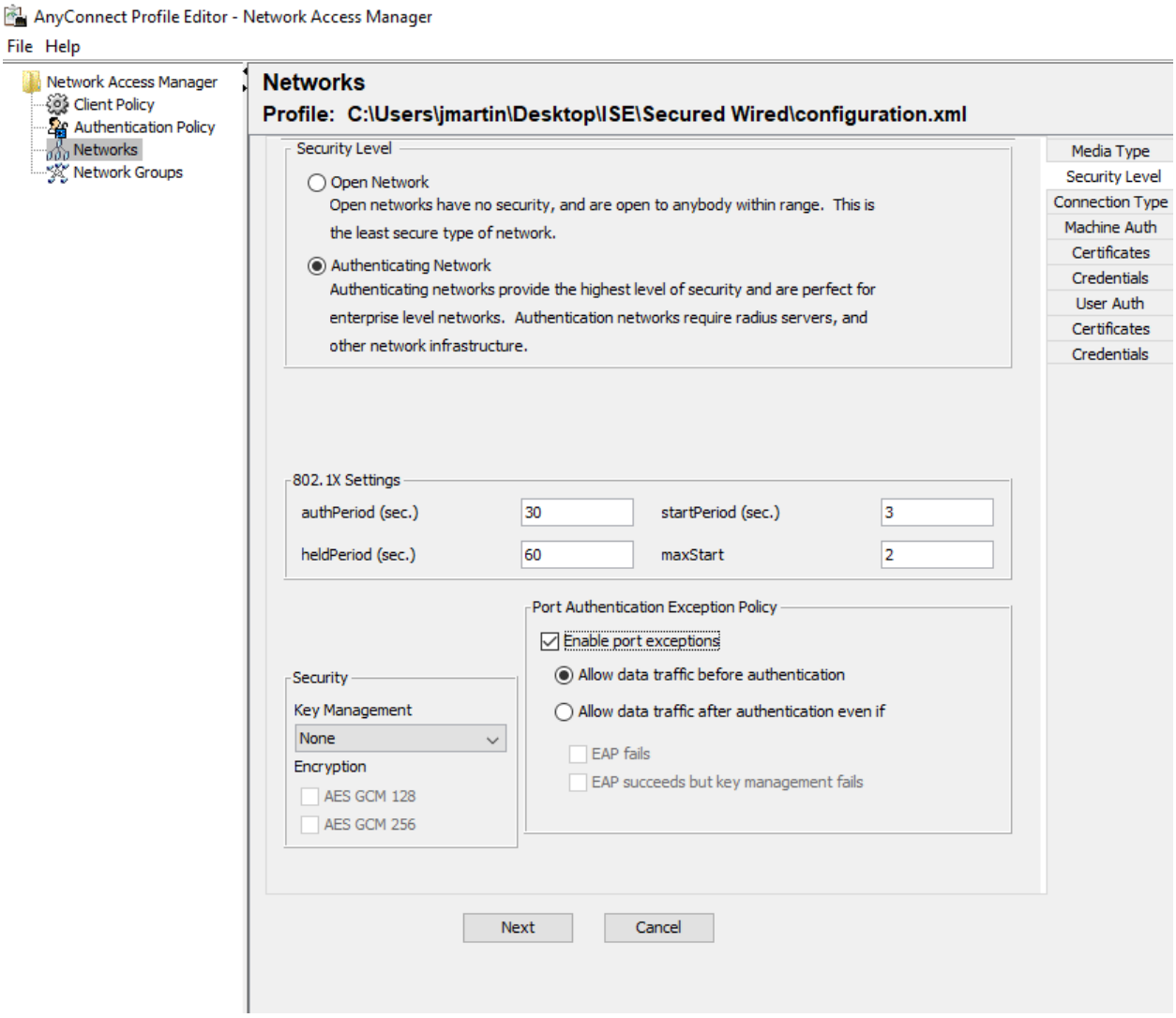
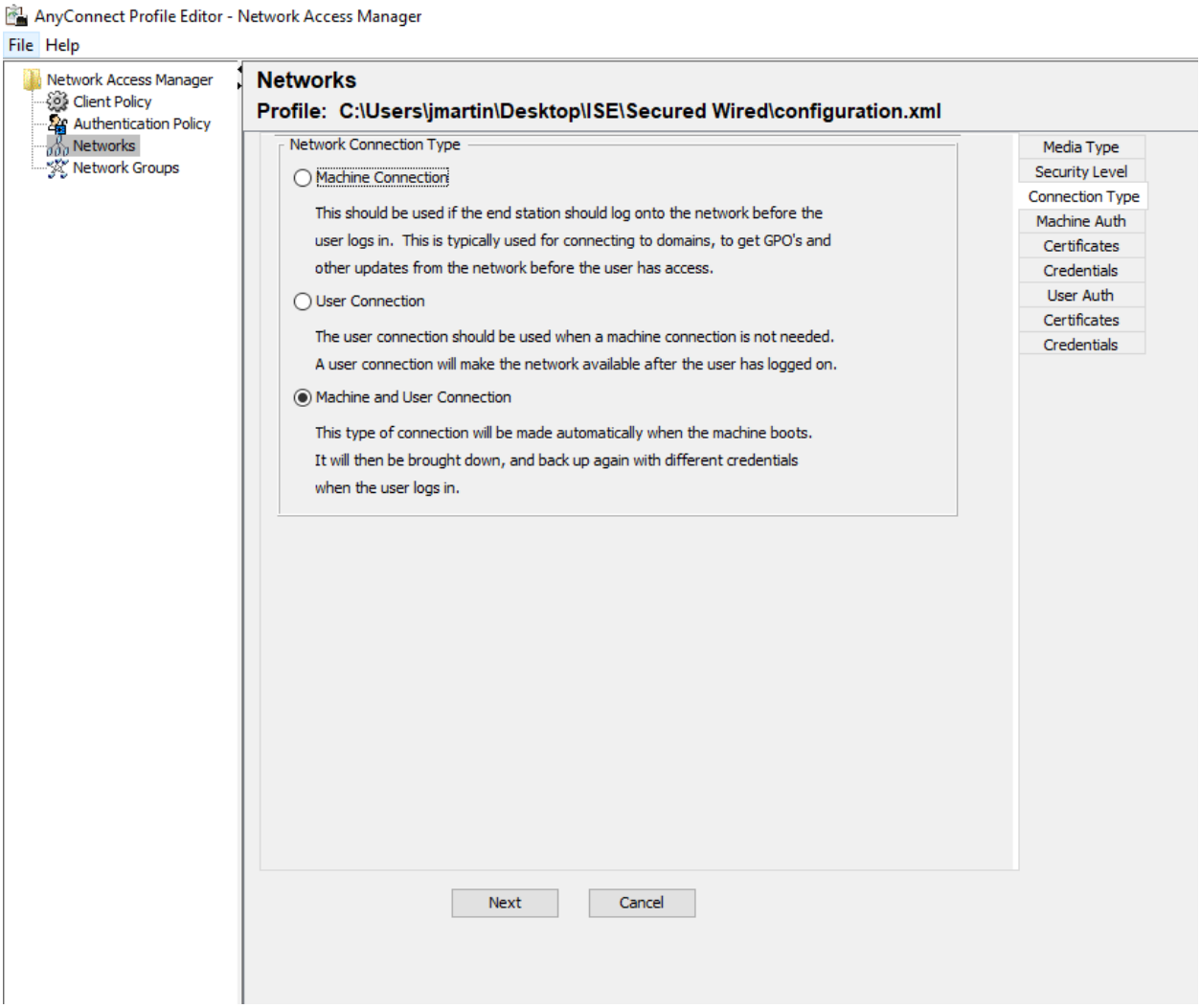
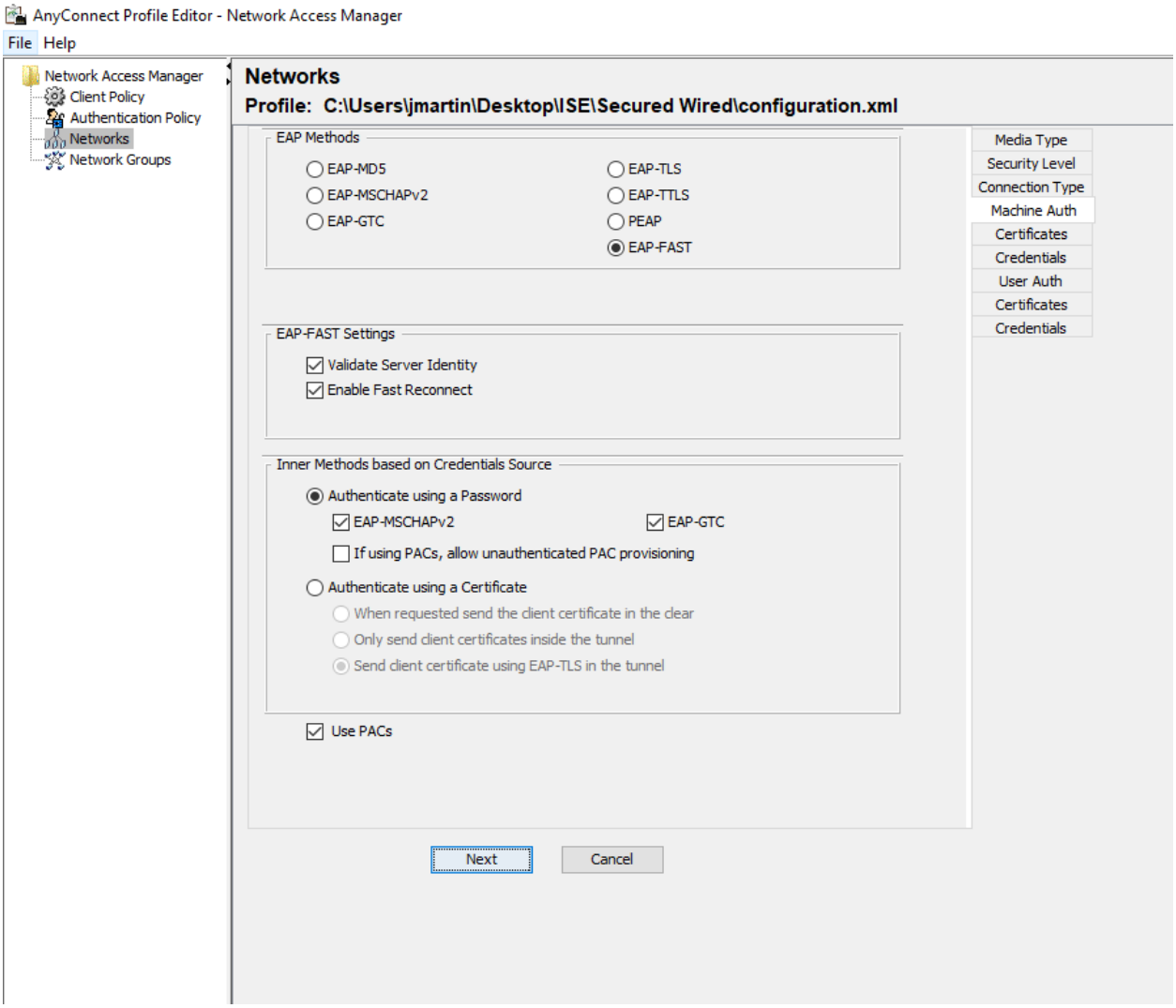

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Client Policy
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Connection Settings
Default Connection Timeout (sec.)
40
Connection Attempt:
Before user logon
Time to wait before allowing user to logon (sec.)
40
After user logon
Media
Manage Wi-Fi (wireless) Media
Enable validation of WPA/WPA2 handshake
Default Association Timeout (sec.)
5
Manage Wired (802.3) Media
Manage Mobile Broadband (3G) Media
Enable Data Roaming
End-user Control
Allow end-user to:
Disable Client
Display user groups
Specify a script or application to run when connected
Auto-connect
Administrative Status
Service Operation
Enable
Disable
FIPS Mode
Enable
Disable

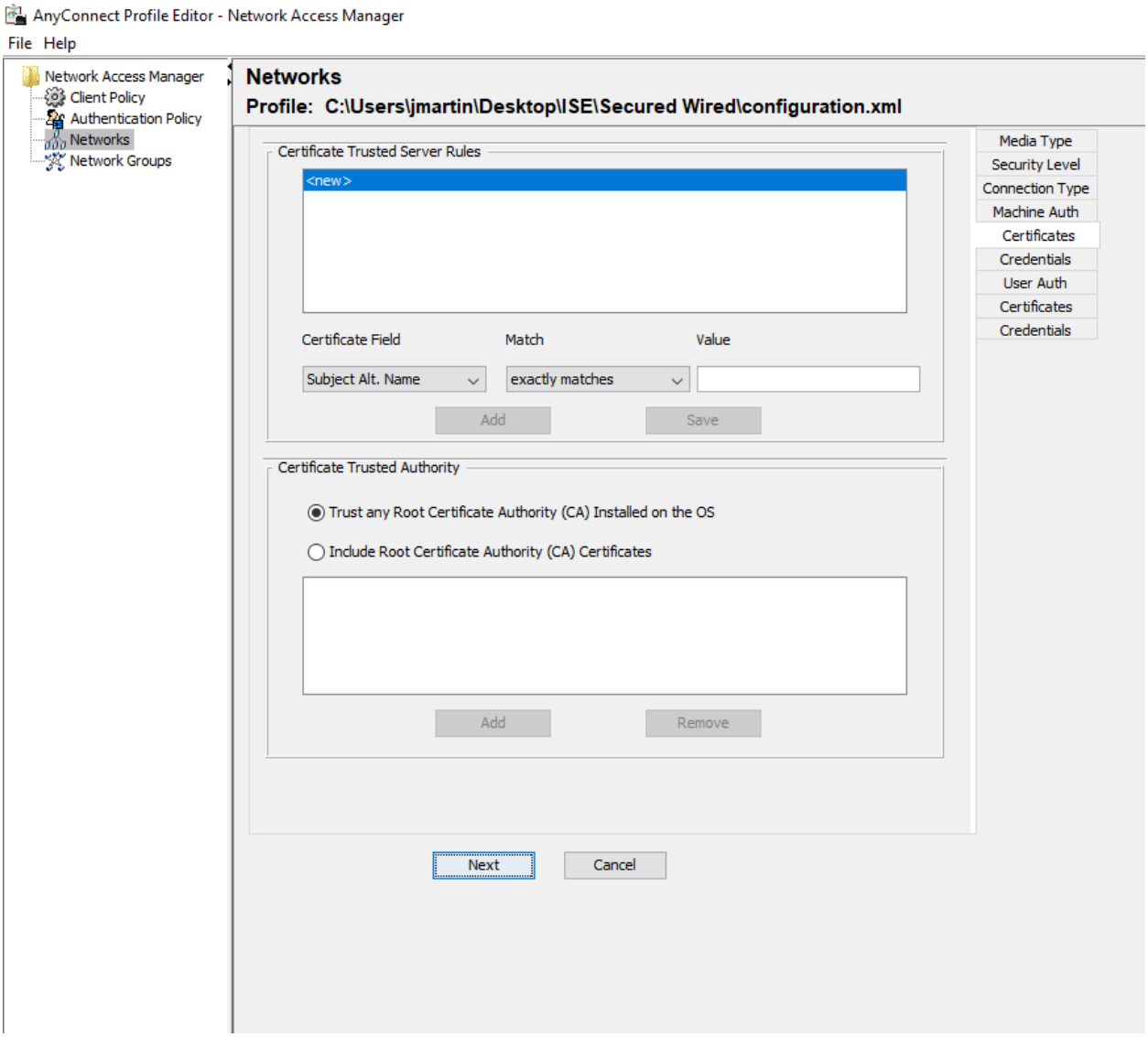

File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Authentication Policy
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Allow Association Modes
Select All (Personal)
Open (no encryption)
Open (Static WEP)
Shared (WEP)
WPA Personal TKIP
WPA Personal AES
WPA2 Personal TKIP
WPA2 Personal AES
Select All (Enterprise)
Open (Dynamic (802.1X) WEP)
WPA Enterprise TKIP
WPA Enterprise AES
WPA2 Enterprise TKIP
WPA2 Enterprise AES
CCKM Enterprise TKIP
CCKM Enterprise AES
Allowed Authentication Modes
Select All Outer
EAP-FAST
EAP-GTC
EAP-MSCHAPv2
EAP-TLS
EAP-TLS
EAP-TTLS
EAP-MD5
EAP-MSCHAPv2
PAP (legacy)
CHAP (legacy)
MSCHAP (legacy)
MSCHAPv2 (legacy)
LEAP
PEAP
EAP-GTC
EAP-MSCHAPv2
EAP-TLS
Allowed Wired Security
Select All
Open (no encryption)
802.1x only
802.1x with MacSec
AES-GCM-128
AES-GCM-256

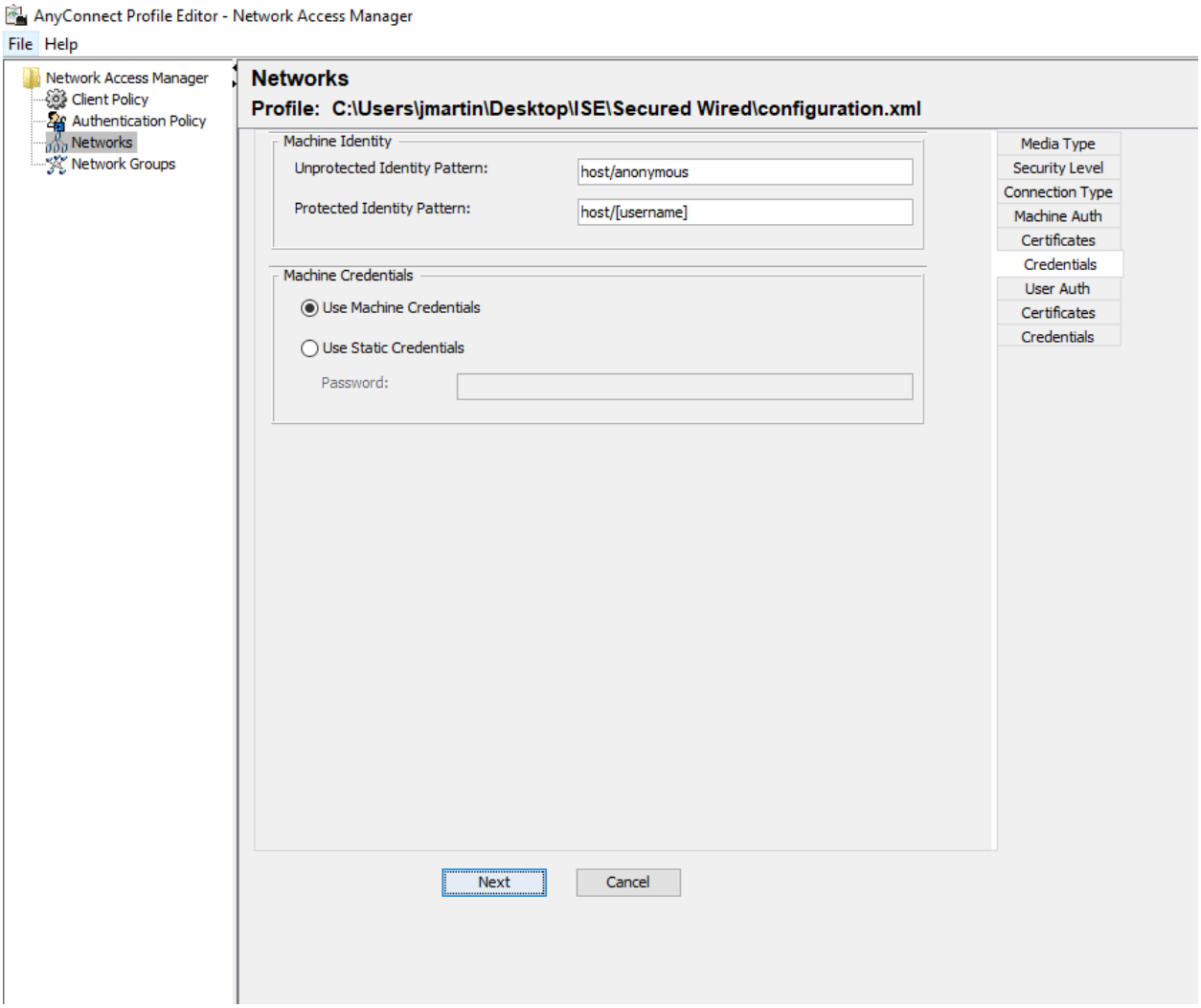

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Name:
ToM_Wired
Group Membership
In group:
Local networks
In all groups (Global)
Choose Your Network Media
Wired (802.3) Network
Select a wired network if the endstations will be connecting to the network with a traditional ethernet cable.
Wi-Fi (wireless) Network
Select a WiFi network if the endstations will be connecting to the network via a wireless radio connection to an Access Point.
SSID (max 32 chars):
Hidden Network
Corporate Network
Association Timeout
5
seconds
Common Settings
Script or application on each user's machine to run when connected.
Browse Local Machine
Connection Timeout
30
seconds
Next
Cancel
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

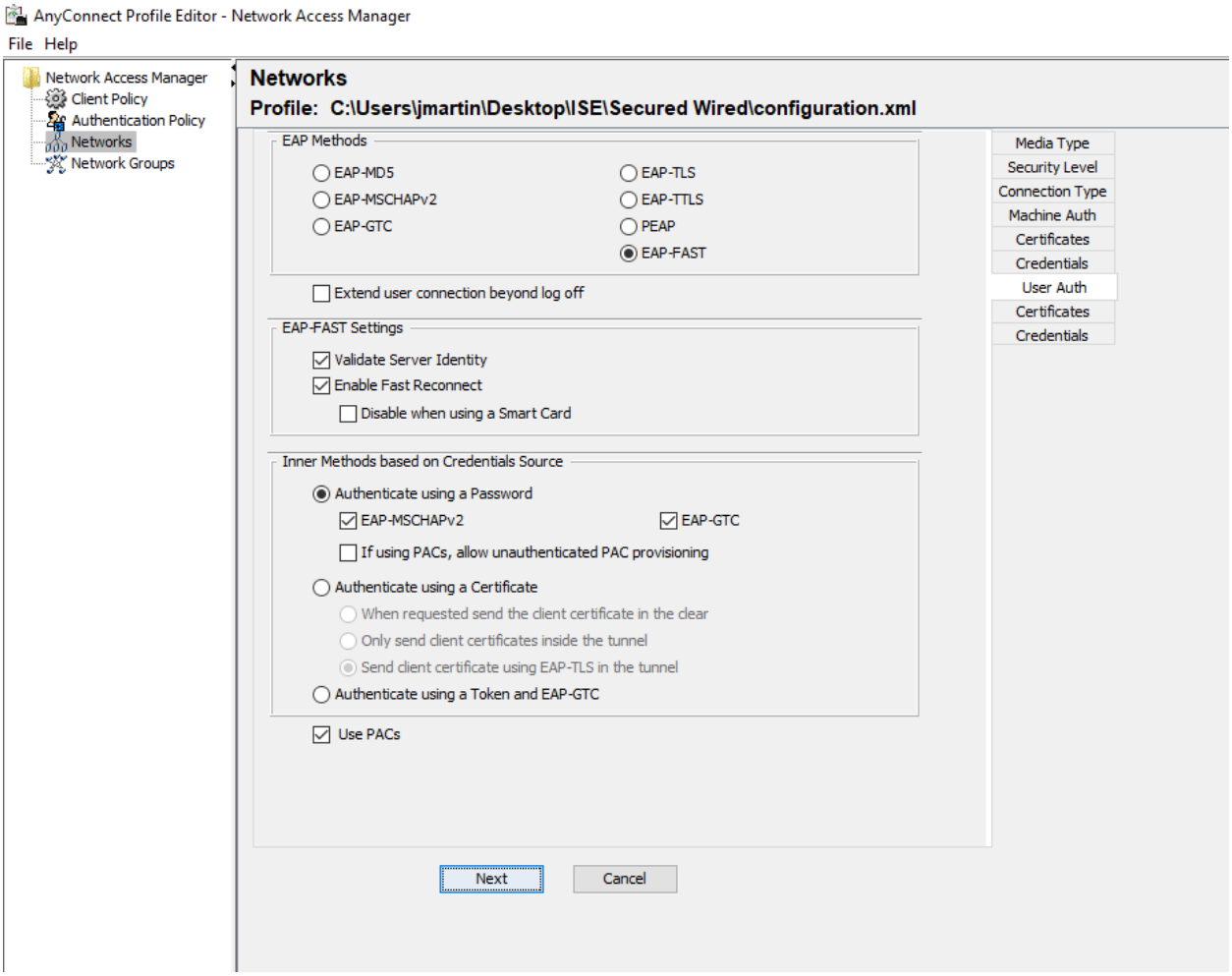

AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Security Level
Open Network
Open networks have no security, and are open to anybody within range. This is the least secure type of network.
Authenticating Network
Authenticating networks provide the highest level of security and are perfect for enterprise level networks. Authentication networks require radius servers, and other network infrastructure.
802.1X Settings
authPeriod (sec.)
30
startPeriod (sec.)
3
heldPeriod (sec.)
60
maxStart
2
Port Authentication Exception Policy
Enable port exceptions
Allow data traffic before authentication
Allow data traffic after authentication even if
EAP fails
EAP succeeds but key management fails
Security
Key Management
None
Encryption
AES GCM 128
AES GCM 256
Next
Cancel
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials

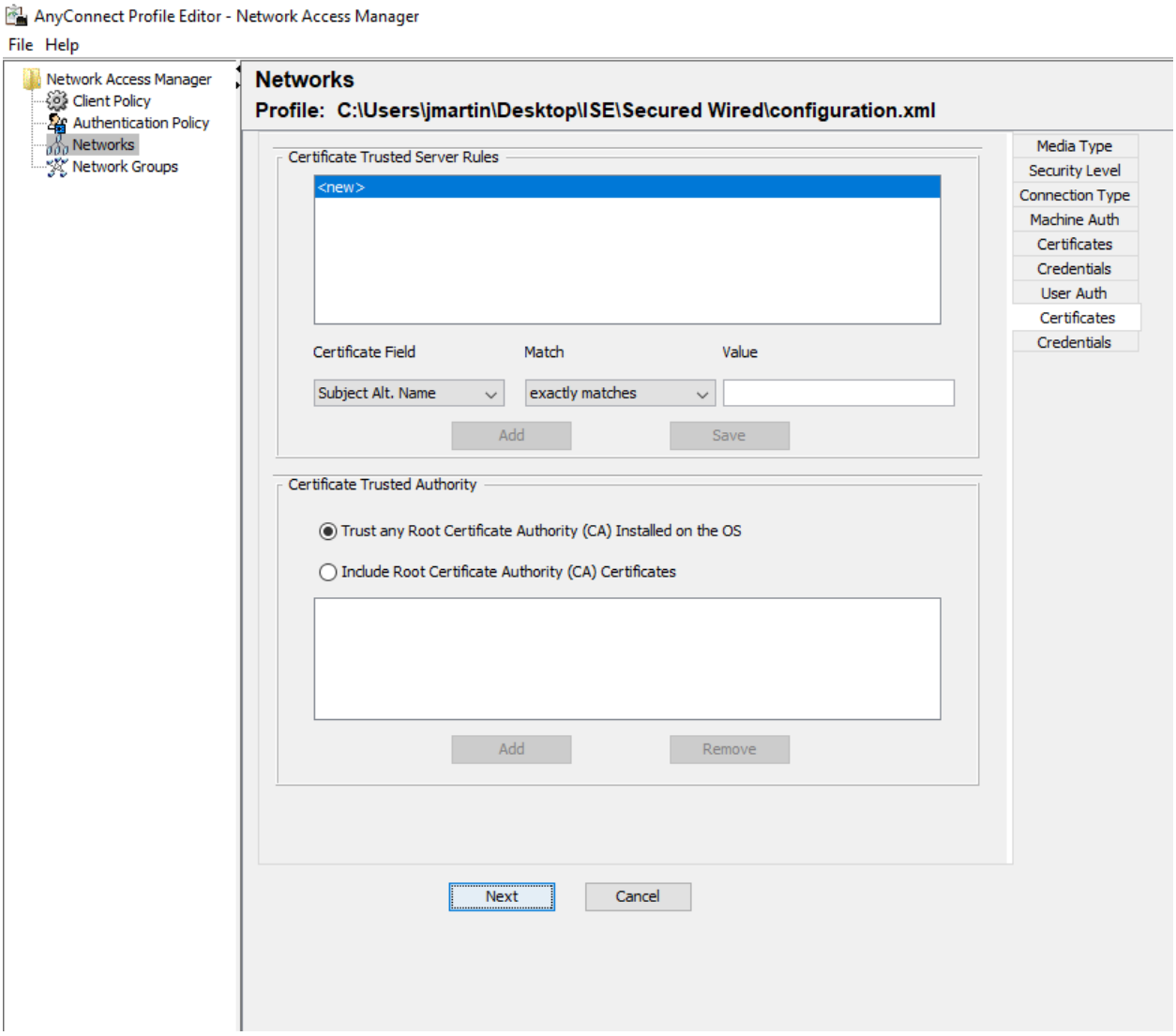

AnyConnect Profile Editor - Network Access Manager
File
Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Network Connection Type
Machine Connection
This should be used if the end station should log onto the network before the user logs in. This is typically used for connecting to domains, to get GPO's and other updates from the network before the user has access.
User Connection
The user connection should be used when a machine connection is not needed. A user connection will make the network available after the user has logged on.
Machine and User Connection
This type of connection will be made automatically when the machine boots. It will then be brought down, and back up again with different credentials when the user logs in.
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Next
Cancel

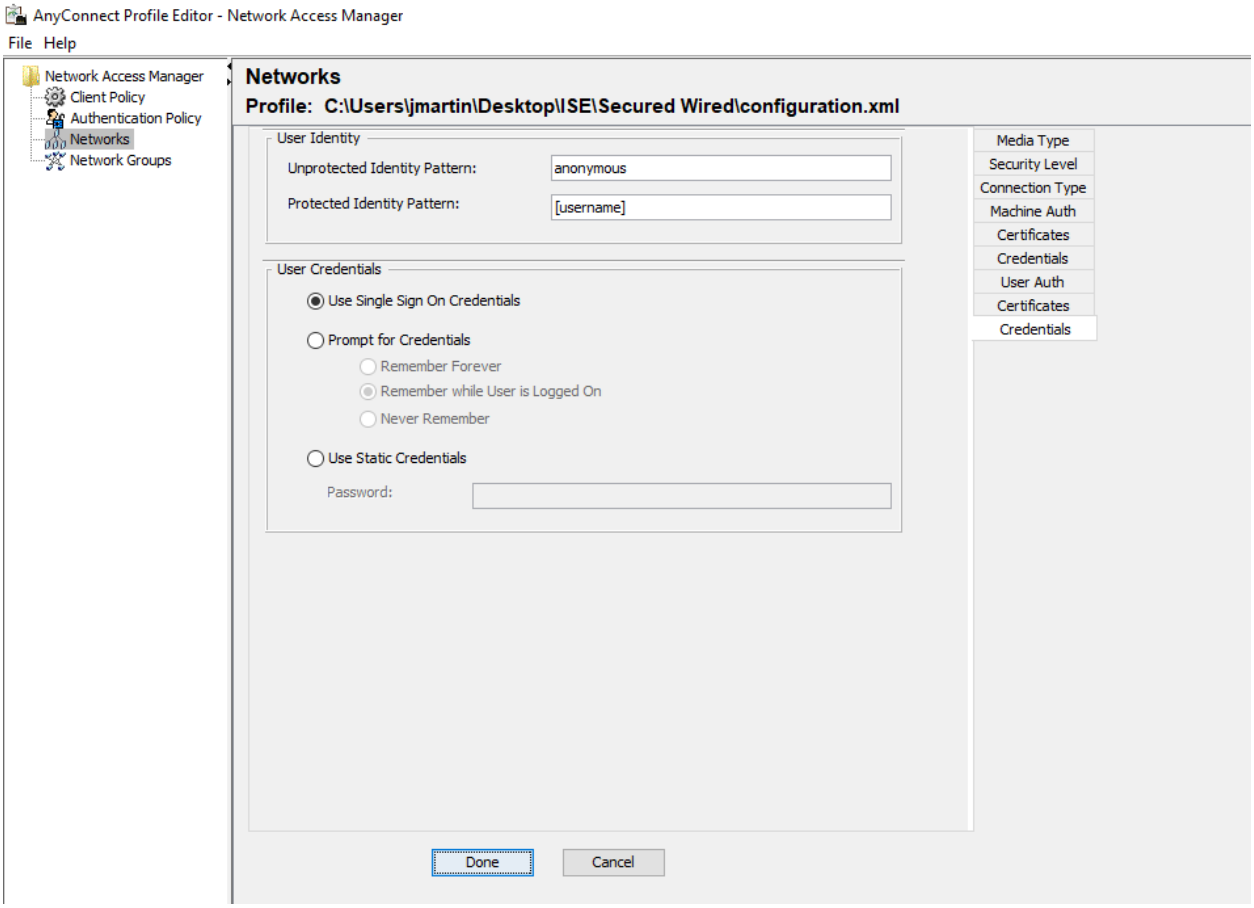

AnyConnect Profile Editor - Network Access Manager
File
Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
EAP Methods
EAP-MD5
EAP-MSCHAPv2
EAP-GTC
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
EAP-FAST Settings
Validate Server Identity
Enable Fast Reconnect
Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
EAP-GTC
If using PACs, allow unauthenticated PAC provisioning
Authenticate using a Certificate
When requested send the client certificate in the clear
Only send client certificates inside the tunnel
Send client certificate using EAP-TLS in the tunnel
Use PACs
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Certificate Trusted Server Rules
<new>
Certificate Field
Match
Value
Subject Alt. Name
exactly matches
Add
Save
Certificate Trusted Authority
Trust any Root Certificate Authority (CA) Installed on the OS
Include Root Certificate Authority (CA) Certificates
Add
Remove
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File
Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Machine Identity
Unprotected Identity Pattern:
host/anonymous
Protected Identity Pattern:
host/[username]
Machine Credentials
Use Machine Credentials
Use Static Credentials
Password:
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
EAP Methods
EAP-MD5
EAP-MSCHAPv2
EAP-GTC
EAP-TLS
EAP-TTLS
PEAP
EAP-FAST
Extend user connection beyond log off
EAP-FAST Settings
Validate Server Identity
Enable Fast Reconnect
Disable when using a Smart Card
Inner Methods based on Credentials Source
Authenticate using a Password
EAP-MSCHAPv2
EAP-GTC
If using PACs, allow unauthenticated PAC provisioning
Authenticate using a Certificate
When requested send the client certificate in the clear
Only send client certificates inside the tunnel
Send client certificate using EAP-TLS in the tunnel
Authenticate using a Token and EAP-GTC
Use PACs
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
Certificate Trusted Server Rules
<new>
Certificate Field
Match
Value
Subject Alt. Name
exactly matches
Add
Save
Certificate Trusted Authority
Trust any Root Certificate Authority (CA) Installed on the OS
Include Root Certificate Authority (CA) Certificates
Add
Remove
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Next
Cancel


AnyConnect Profile Editor - Network Access Manager
File Help
Network Access Manager
Client Policy
Authentication Policy
Networks
Network Groups
Networks
Profile: C:\Users\jmartin\Desktop\ISE\Secured Wired\configuration.xml
User Identity
Unprotected Identity Pattern:
anonymous
Protected Identity Pattern:
[username]
User Credentials
Use Single Sign On Credentials
Prompt for Credentials
Remember Forever
Remember while User is Logged On
Never Remember
Use Static Credentials
Password:
Media Type
Security Level
Connection Type
Machine Auth
Certificates
Credentials
User Auth
Certificates
Credentials
Done
Cancel