Secure Communications Clients - Host

Secure Communications between UA-Clients and UA-Host

Uniface Anywhere provides support for both Transmission Control Protocol (TCP) and Secure Socket Layer (SSL) as methods for communication between Windows and Uniface Anywhere Hosts.

Host Administrators can optionally encrypt all data transmitted between the client and the host. This includes the client’s user name and password, which are supplied during logon, and any application data submitted by the client or returned by the host.

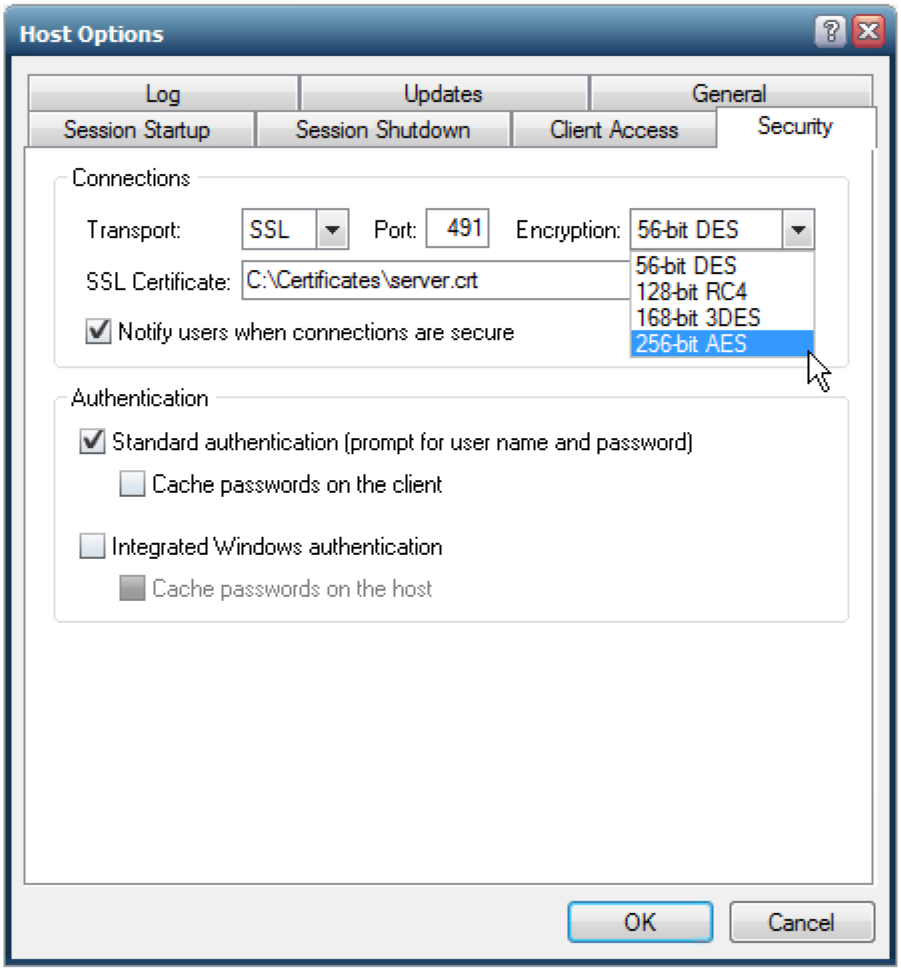
When TCP transport mode is selected, Uniface Anywhere uses 56-bit DES encryption by default setting. The DES key is exchanged using RSA Public-Key Cryptography Standards. The RSA keys are 512-bits.

When selecting the SSL transport mode:

1. An SSL Certificate file must be specified. SSL certificates are required to secure communication between Uniface Anywhere clients and hosts.
2. The following encryption algorithms are also available: 128-bit RC4, 168-bit 3DES, and 256-bit AES.
   A special license (StrongEncryption) is required to use these algorithms. To obtain this license, contact your Uniface Sales representative or mail Uniface License Management.

How to change Communication protocol / encryption

Changing the Transport Protocol and its Encryption can be done on the Uniface Anywhere Host by the UA Administrator in the UA Cluster Manager / Admin Console - Tools - Host Options... - 'Security' Tab page.



Connections

Transport: SSL Port: 491 Encryption: 56-bit DES

SSL Certificate: C:\Certificates\server.crt

☑ Notify users when connections are secure

Authentication

☑ Standard authentication (prompt for user name and password)

□ Cache passwords on the client

□ Integrated Windows authentication

□ Cache passwords on the host

How to get an SSL Certificate

You can obtain a certificate from a trusted Certificate Authority (CA) such as Verisign or Thawte, or you can create your own certificate authority and then sign your server certificates from this authority. Wildcard SSL certificates are also supported.

In the Uniface Anywhere Administrator Guide, you'll find the next chapters (starting at page 42) on how to create certificates that can be used by Uniface Anywhere:

- Obtaining a Trusted Server Certificate
- Using an Intermediary SSL Certificate
- Creating Your Own Certificate Authority
- Creating a CA Key and Certificate
- Creating and Signing Server Keys
- Generating a CSR Using IIS Certificate Wizard
- Active Directory Certificate Services (AD CS) (Not in the administrator guide, but can be found here)

Be notified that Uniface Anywhere can only support Certificates in the PEM format. It happens that systems or third-party CA's deliver certificates in the DER format.
In the Uniface Anywhere Administrator Guide, you can find a procedure to convert DER formatted files to PEM formatted files using Openssl.

Which files are required for SSL transport

When using Trusted Server Certificate or Intermediary Certificate, then the files '`server.crt`' and '`server.key`' are required.
The server key and certificate files (e.g., `server.key` and `server.crt`) must have the same base filename and be located in the same directory on the Uniface Anywhere Host.

When using your Own Certificate Authority (self signed certificates) you will also need file '`ca.crt`' in the same directory on the Uniface Anywhere Host.

All these files need to be copied in a directory on the target server that can be accessed from the System account but cannot be accessed from the accounts of users who will sign in to the host.

<< UA Technical Information