



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at <http://www.giac.org/registration/gsec>

What is Secure Outlook Web Access (SSL-OWA)?

Cliff Rittel

September 13, 2000

What is OWA?

Microsoft OWA for Exchange Server offers the ability to access secure e-mail, calendar, scheduling and collaboration applications using the Internet Explorer Web Browser. A server running Exchange 5.5 and Internet Information Server are required on the backend. The IIS server uses active server pages to handle the requests and interact with the central log on server for authenticity and the Exchange Information Store for access to a mailbox. Mailbox information can only be accessed while client/server on-line connectivity exists. This application is used primarily as a central server application service, which remote clients connect to over the public Internet. Due to the inherent insecurity of the Internet, security settings such as SSL need to be put in place.

What is ASP and SSL?

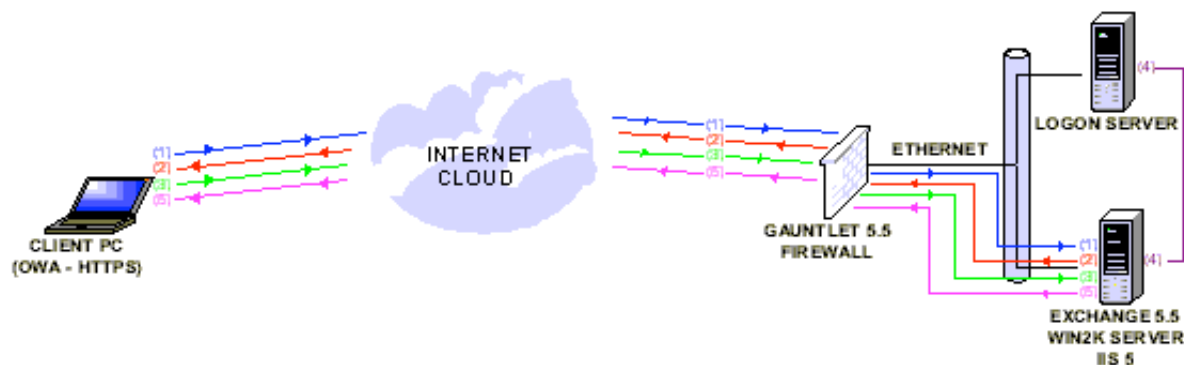
ASP is an acronym for Application Server Provider and refers to an environment where clients access a central server over the Internet, and the core data resides on the server. The OWA connection fits the ASP model because all of the data is centrally hosted and decentralized clients are accessing the data. Typically, ASP

SSL is an acronym for Secure Sockets Layer which is a protocol developed by Netscape Communications to provide secure data transmissions over the Internet. SSL is a transport layer security technique that can be applied to HTTP and provide privacy between two communicating devices, as this paper will demonstrate the Windows client and the Exchange/IIS server. SSL provides mandatory authentication, encryption and data integrity. The protocol mandates data transmissions by a session key so that data transmissions cannot be altered or disclosed. A more in depth understanding of the SSL transaction will be established in the next sections.

Setup of OWA

For my test, I used Windows clients (98/NT/2000) connected to dial up, cable modem and T1 connections over the Internet to illustrate the ASP functionality. Please note IE is required as OWA connectivity will not work with Netscape or any other Internet Browser. I used NAI's Gauntlet 5.5 firewall and built a proxy to handle the connection. On the LAN, I used a standard Intel server configuration running Windows2000 SP1, Exchange 5.5 SP3 and IIS 5. For SSL I used a server certificate issued by a publicly trusted root CA, Thawte, and installed it on the IIS server. I only required server side authentication, but to add an additional layer of authentication security one could require the client have a valid SSL certificate (see IIS SSL ENABLE SETUP). Below is a diagram of the network topology, screen shots of the log on transaction and further explanation of the SSL/OWA and network authentication transaction.

Client/Server SSL - OWA Setup & Network Authentication



SSL Transaction

In order for the SSL transaction to work both the client (IE) and the Server (IIS) must be SSL enabled. The transaction runs over TCP. (1) The security transaction begins when the client sends a request to the server for its digital certificate. Traditionally, this begins with typing https: in the URL locator. (2) The server sends its digital

certificate to the client. The client will check the digital certificate for accuracy in terms of issuance from a trusted root Certificate Authority, valid date on the certificate and common name of the certificate. If there are any problems the user has the option to view the certificate, continue or cancel the transaction. (3) If the client continues, then the client authenticates the server by decrypting the digital signature that is within the digital certificate. The client then generates a session key and encrypts it using the server's public key from the certificate sends it to the server. Once the server receives the session key it uses it to encrypt and decrypt the data tunnel. SSL uses message authentication to ensure tampering with data transferred between the client and server has not taken place.

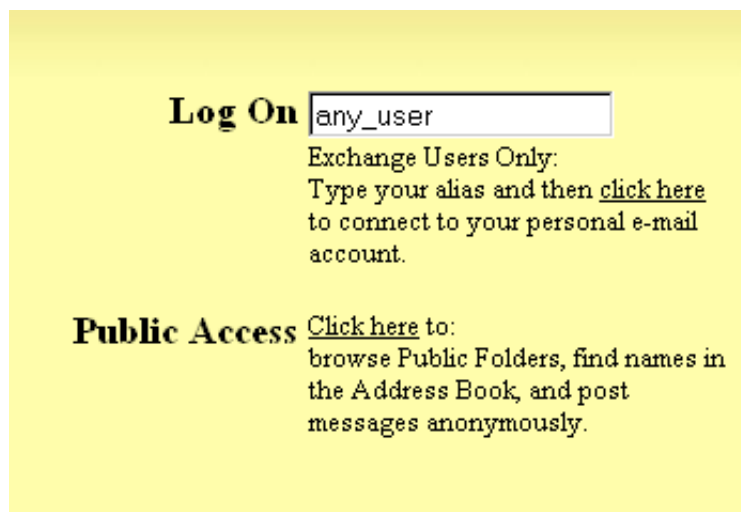
Example (2)



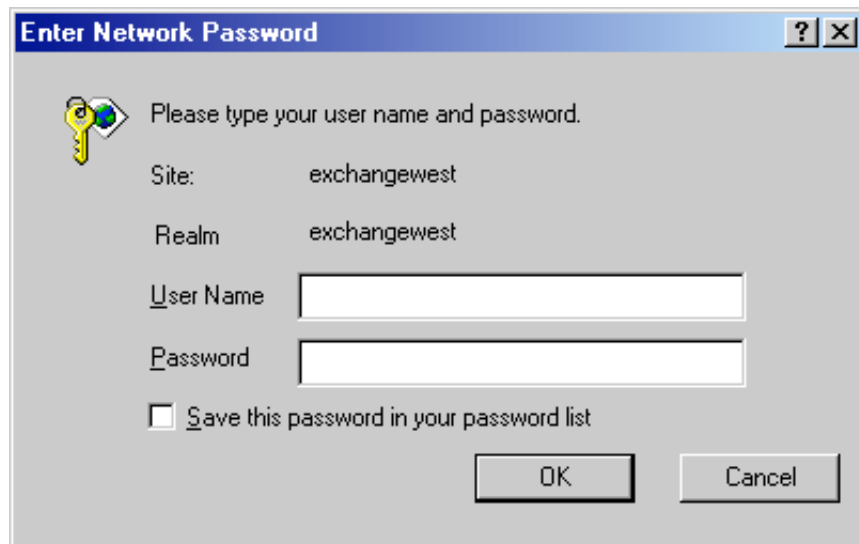
Logon Authentication

Once the SSL session is established between the client and server, the server requests from the client a user alias mailbox on the client. (4) Then the client is prompted for its network logon credentials, which it then authenticates with a Logon Server. (5) Once authenticated with a valid user account the Exchange server offers the client access to their mailbox resources.

OWA Log On Mailbox Alias Screen



Network Logon Server Screen (4)



Enter Network Password

Please type your user name and password.

Site: exchangewest

Realm: exchangewest

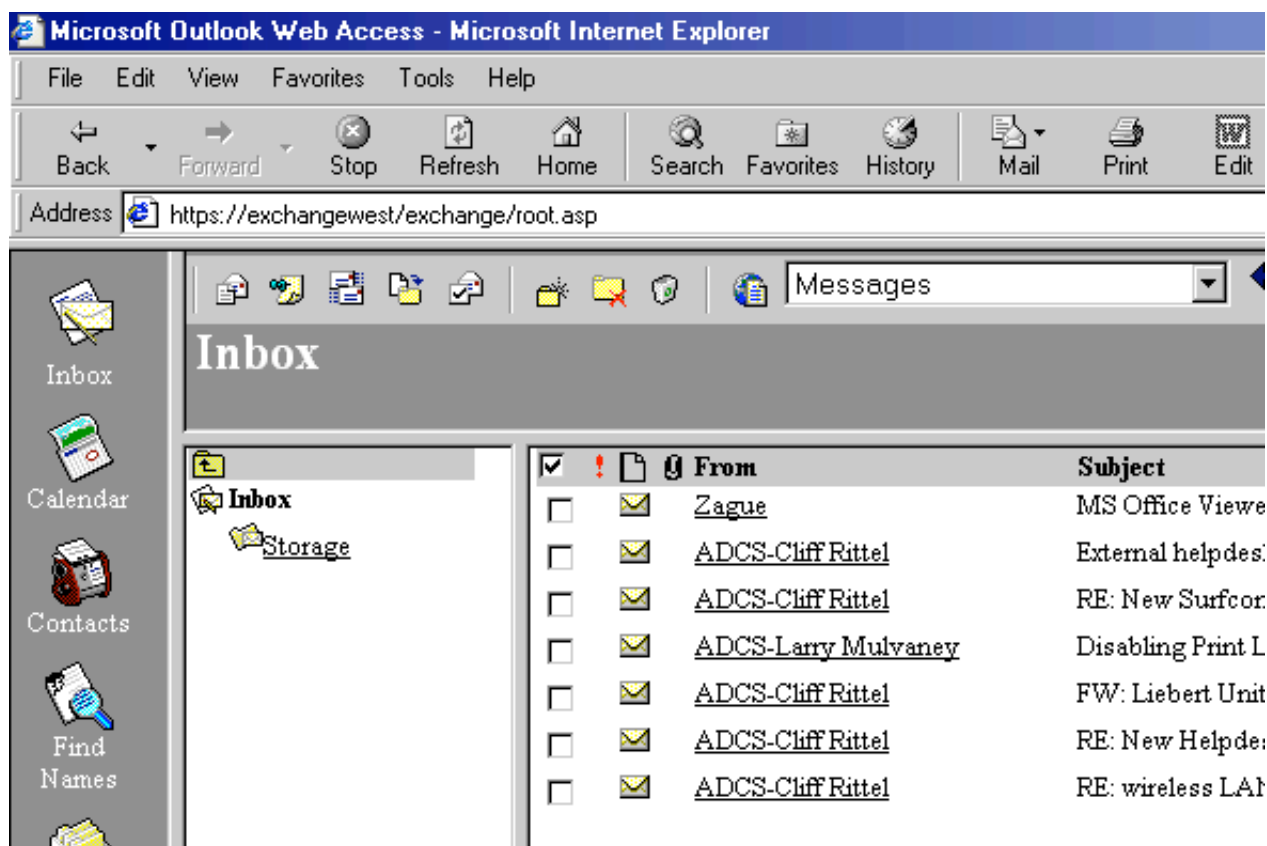
User Name:

Password:

☐ Save this password in your password list

OK Cancel

Mailbox Resource Screen (5)



Microsoft Outlook Web Access - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites History Mail Print Edit

Address <https://exchangewest/exchange/root.asp>

Inbox

Calendar

Contacts

Find Names

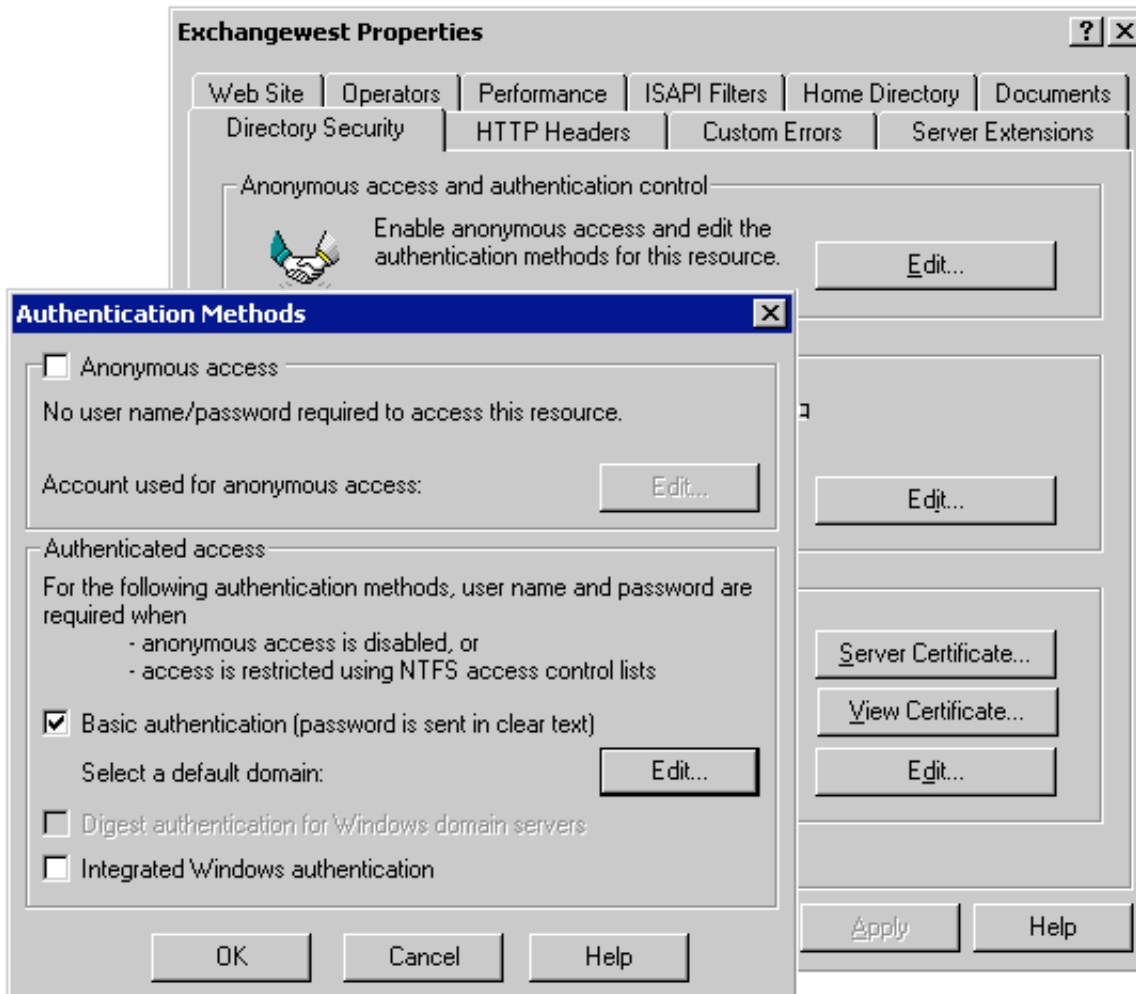
Messages

	From	Subject
<input checked="" type="checkbox"/>	Zague	MS Office Viewe
<input type="checkbox"/>	ADCS-Cliff Rittel	External helpdes
<input type="checkbox"/>	ADCS-Cliff Rittel	RE: New Surfcor
<input type="checkbox"/>	ADCS-Larry Mulvaney	Disabling Print L
<input type="checkbox"/>	ADCS-Cliff Rittel	FW: Liebert Unit
<input type="checkbox"/>	ADCS-Cliff Rittel	RE: New Helpde:
<input type="checkbox"/>	ADCS-Cliff Rittel	RE: wireless LA

IIS SSL Enable Setup

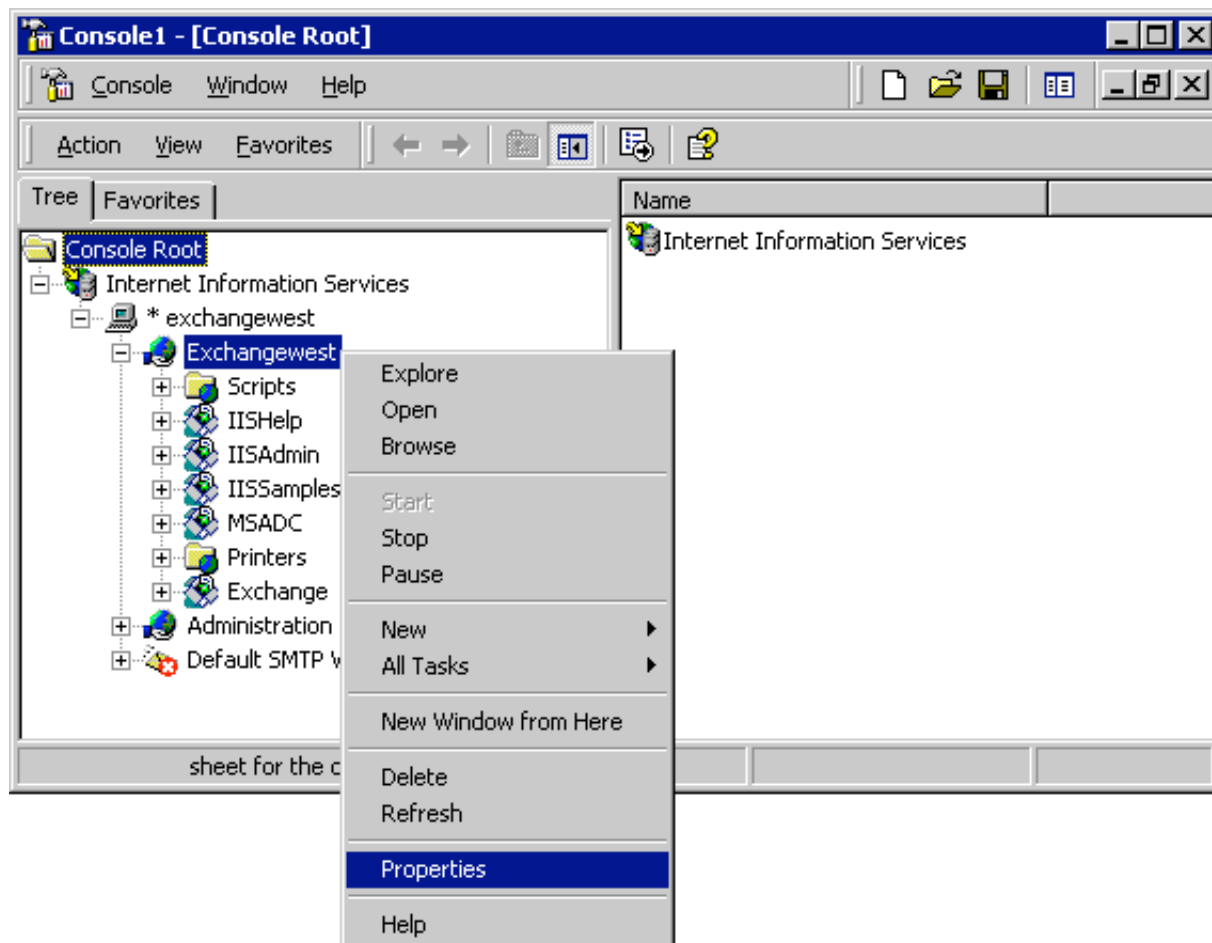
As noted previously, the test installation was on a Windows2000 SP1 platform with Exchange Server 5.5 SP3 and Internet Information Server 5. The following screen shots give a graphical presentation on how to set up SSL within IIS. The SSL connection has additional security options such as requiring the browser to establish 128 bit encryption or mandating client certificates.

Properties of IIS Web Server

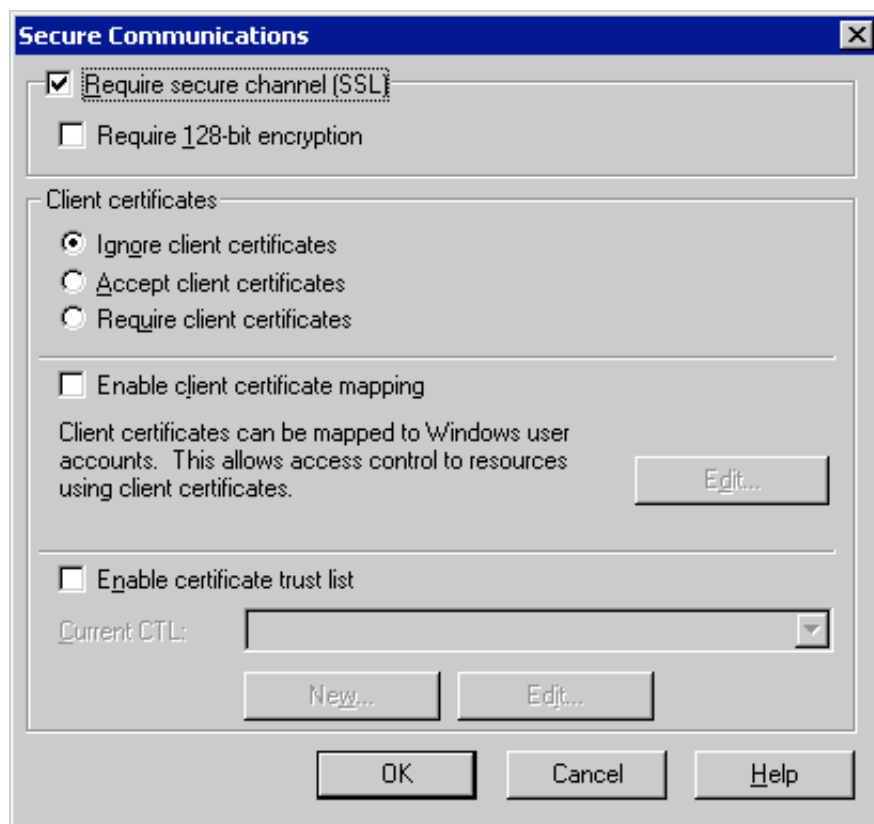


Manage Secure Communications

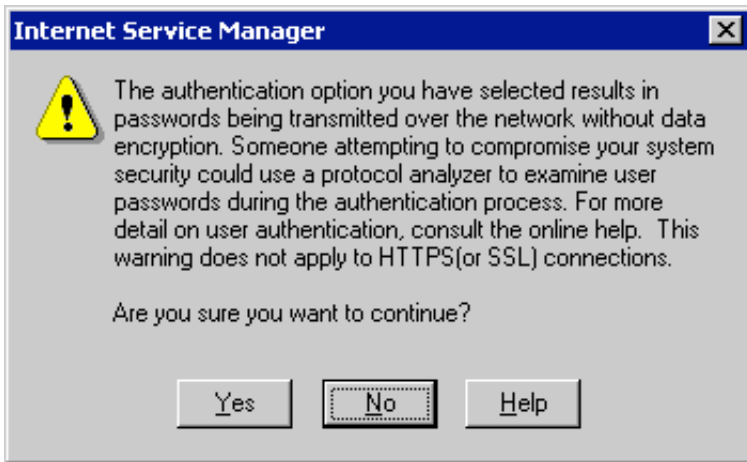
© SANS Institute



Very important security warning message



This screen shows SSL connection options.



Conclusion

OWA over a SSL connection can offer an effective, secure communication over the public Internet to an Exchange mailbox. OWA operates as an ASP host, which increases the ability to tighten security in a central location. OWA installations without SSL are a security risk as users will send their passwords in clear text over the Internet. SSL ensures authentication, encryption and data integrity. When establishing any type of remote access into an internal network a well thought out plan is essential to ensure the highest level of security possible in protecting precious Information Systems.

References

Microsoft Corporation. (1999). "Planning and Deploying Outlook Web Access 5.5". Microsoft Corporation. Redmond, WA. White Paper.

Microsoft Corporation (1999). "ASP Certification White Paper". Microsoft Corporation. Redmond, WA.
<http://www.microsoft.com/ISN/downloads/ASP%20Certification%20White%20Paper.doc> White Paper.

Minoli, Daniel, E. Minoli. (1998). Web Commerce Technology Handbook. McGraw-Hill Companies Inc. New York, NY.

Network Associates Technology, Inc. (1996-1999). Gauntlet Firewall/VPN for WindowsNT Getting Started Guide v5.5. Network Associates Technology, Inc. Santa Clara, CA.

Thawte - A Verisign Company. www.thawte.com

© SANS