YULANE

Network Common User FAQ and Troubleshooting

Unedited – Version 5

Updated 11/10/2016

William Lucking
will@orangerocket.biz

Contents

This document is stored in \\Store\Tech Support. Only users in the Owners security group may access this document.

Obtaining Support

The purpose of this document is to provide answers to frequently asked questions so that Yulane staff do not have to contact Network Support as frequently as they otherwise would.

Yulane will designate only one person to control the technical support issues between all Yulane staff and Network Support. All Yulane support requests should be routed through that person who will directly communicate with Network Support. The designated person will email the issue to Network Support at will@orangerocket.biz. If deemed necessary by Network Support, issues may be moved to QQ chat.

The process for obtaining Network Support follows:

1. Respect the time of Network Support. Spend a few minutes trying to solve your own problem using a Google search. Network Support will do this in order to solve your problem, so should you. In doing so you might find the answer to your question and save yourself and everyone else a lot of time.
2. If a problem remains unsolved, contact the Yulane technical support point of contact with the issue. Maybe that person can run a Google search, reference this FAQ, or use her experience to solve the problem. However, if she is unable she may email Network Support with screenshots, illustrations, and a description of the process used leading to the problem. For the fastest response ensure the description of the problems are detailed. Vague descriptions will lead to a lot of back-and-forth and slow resolution.
3. Network Support will receive the support email and address it once per day. Allow up to 24 hours for a response. Communication will occur through email unless Network Support wishes to take the issue to QQ chat.

VPN

VPN provides a secure communication pipeline between a user and the Yulane network. When connected by VPN the connecting computer may access the resources on the network as if the computer was physically within the local area network.

Unless added to Active Directory, the connecting computer will not have an Active Directory account. However, the user will and therefore Active Directory permissions will apply to the user, but not the computer.

When connected to VPN the Microsoft Remote Routing and Access Service performs access filtering, user authentication, and obtains an IP from the DHCP server that is given to the connecting computer so that the computer may connect within the network. The IP address resides in the 192.168.11.0/26 subnet.

The connecting computer's default gateway should remain unchanged by this process. This means that internet use of the connecting computer will be routed not through the VPN connection, but through the user's regular internet connection.

DNS resolution will occur through the Yulane network. This allows resources in the Yulane domain to be identified.

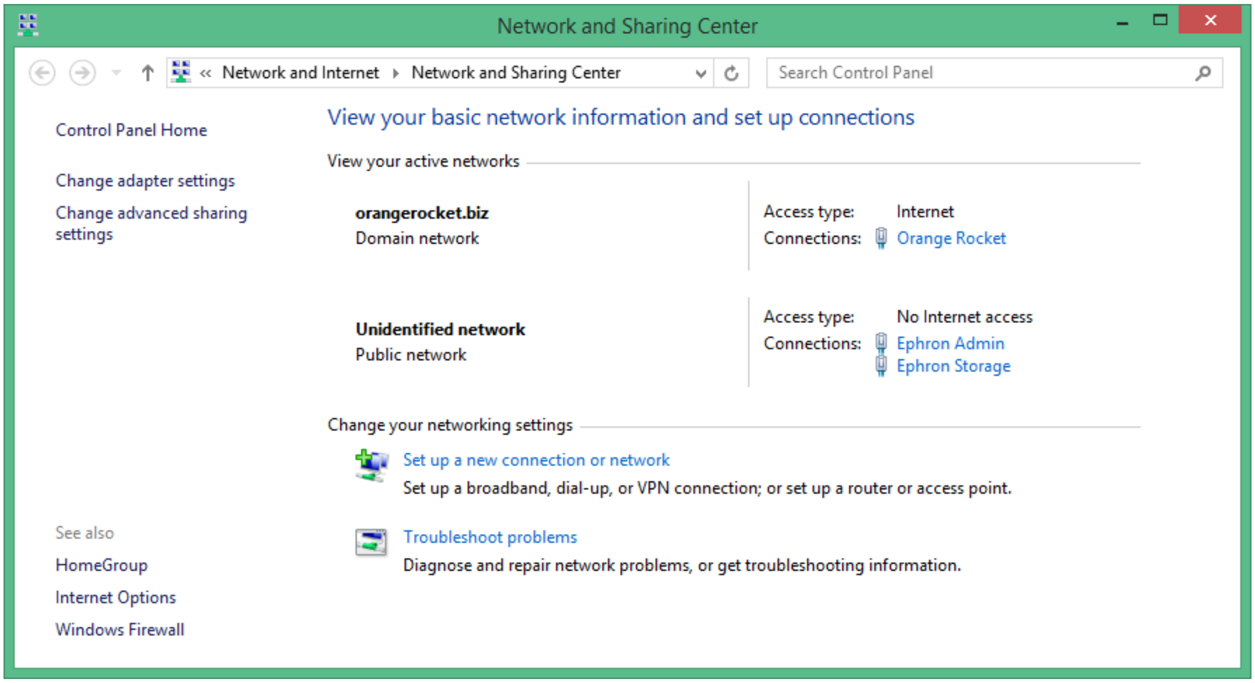
Access Requirements:

Users must be in the Active Directory VPN Users security group.

Connecting

To establish a connection to VPN perform the following (Windows 8.1 sample):

1. Under *Control Panel*, go to *Network and Sharing Center*
2. Select *Set up new connection or network*



View your basic network information and set up connections

View your active networks

orangerocket.biz
Domain network

Access type: Internet
Connections: Orange Rocket

Unidentified network
Public network

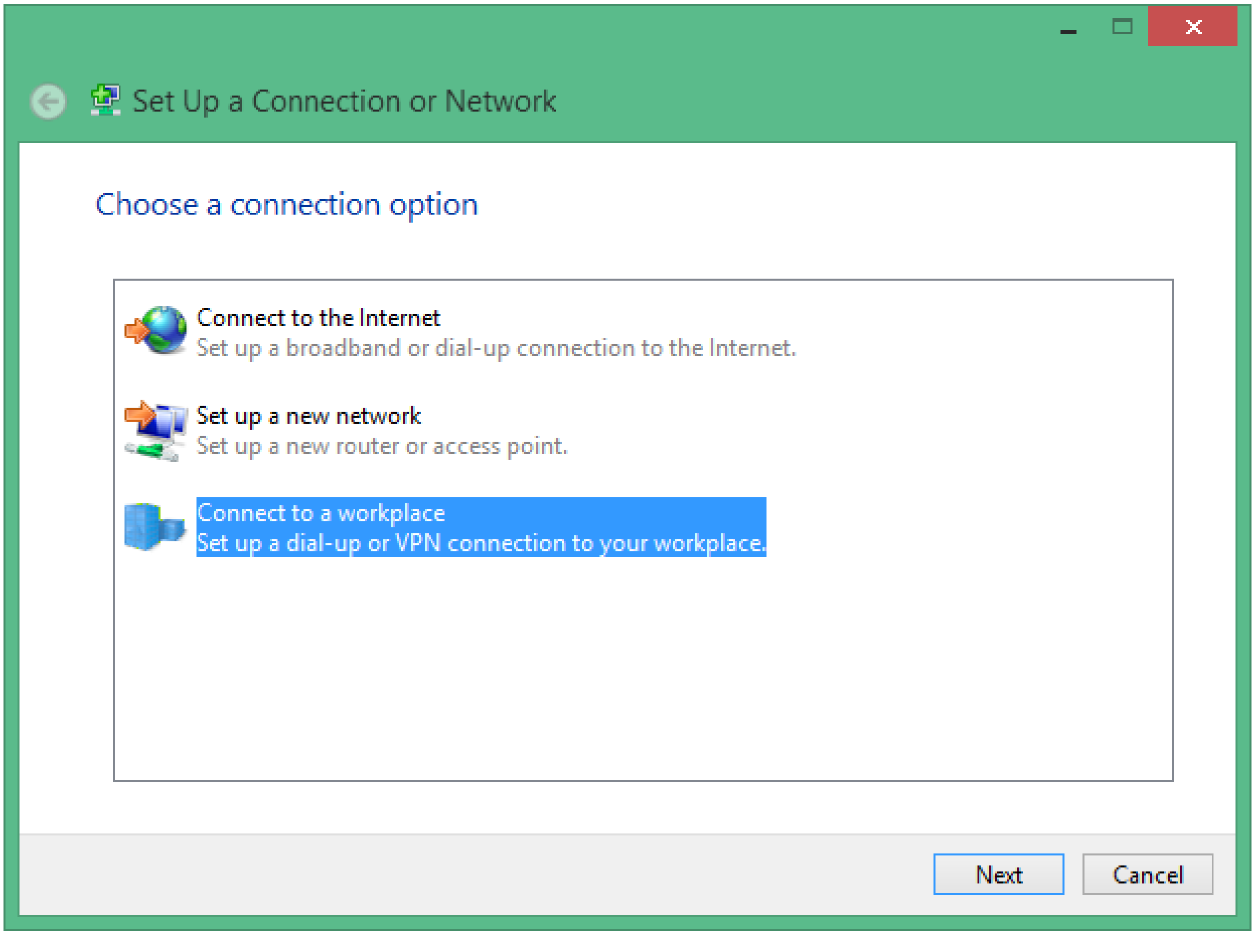
Access type: No Internet access
Connections: Ephron Admin
Ephron Storage

Change your networking settings

Set up a new connection or network
Set up a broadband, dial-up, or VPN connection; or set up a router or access point.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

3. Select *Connect to a workplace*
4. Click Next



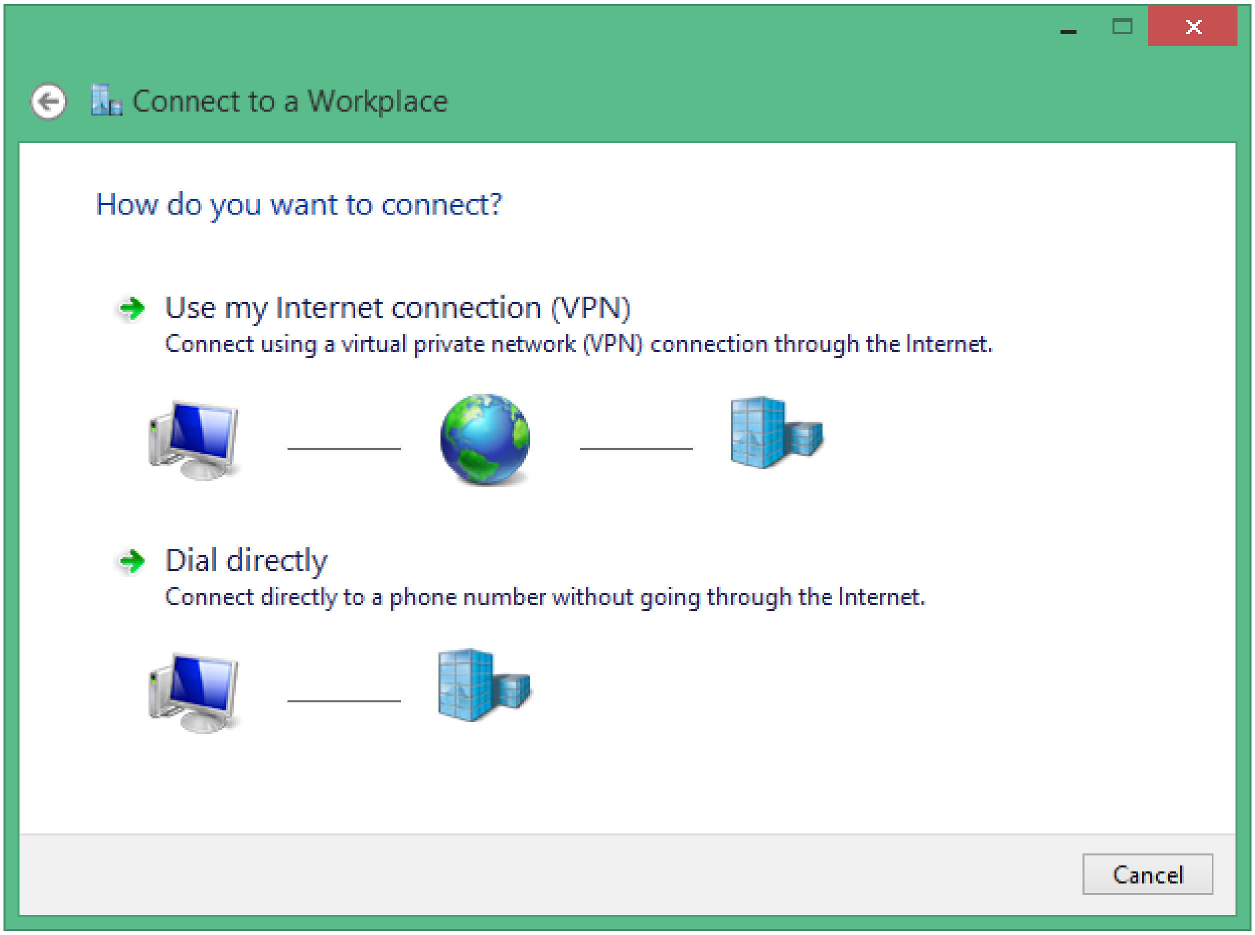
Choose a connection option

Connect to the Internet
Set up a broadband or dial-up connection to the Internet.

Set up a new network
Set up a new router or access point.

Connect to a workplace
Set up a dial-up or VPN connection to your workplace.

5. Click *Use my Internet connection (VPN)*



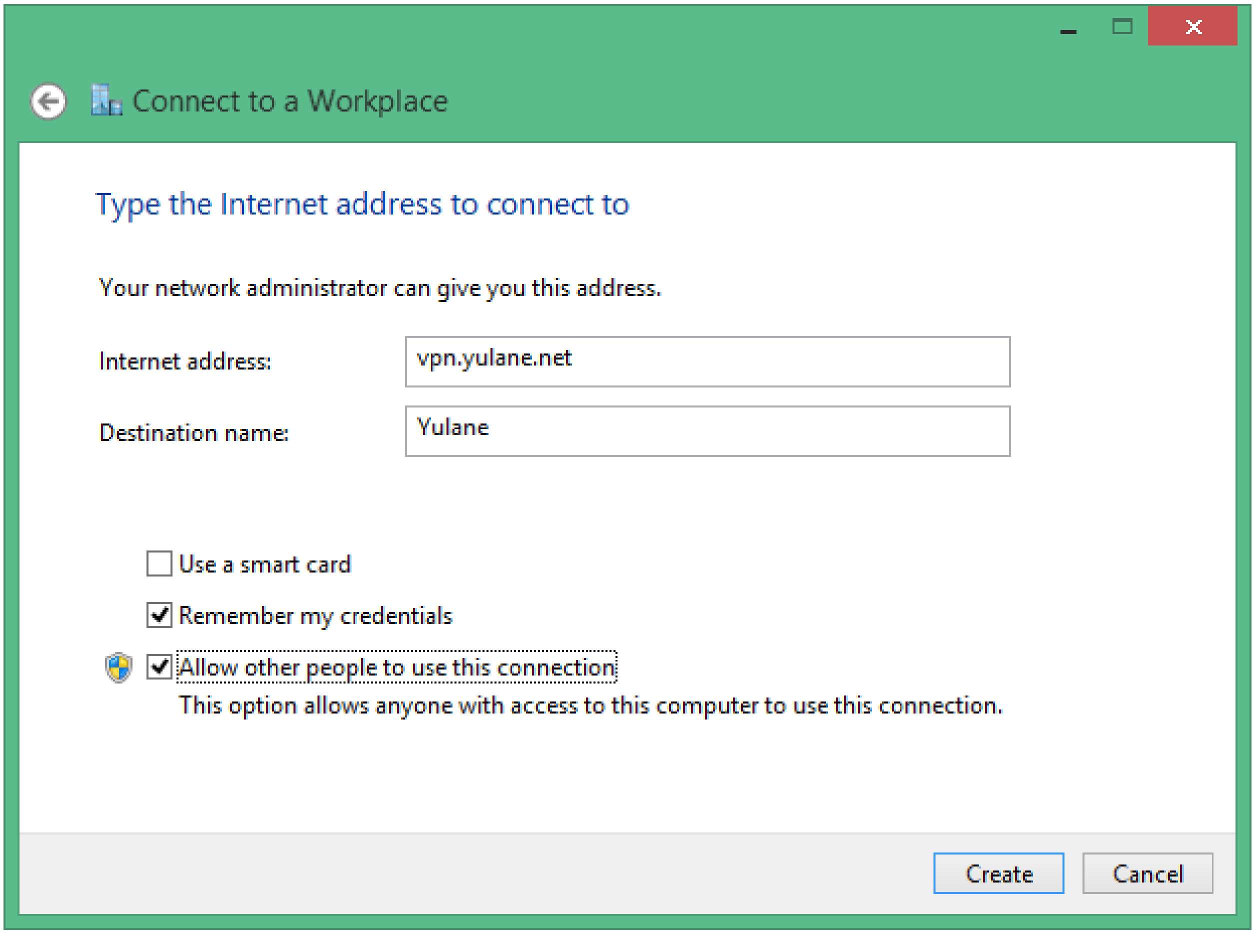
Connect to a Workplace

How do you want to connect?

Use my Internet connection (VPN)
Connect using a virtual private network (VPN) connection through the Internet.

Dial directly
Connect directly to a phone number without going through the Internet.

6. Type vpn.yulane.net for the Internet address and name the connection Yulane. Optionally, select Allow other people to use this connection (necessary if you want to add the computer to the network as some point in the future).
7. Click Create



Type the Internet address to connect to

Your network administrator can give you this address.

Internet address: vpn.yulane.net

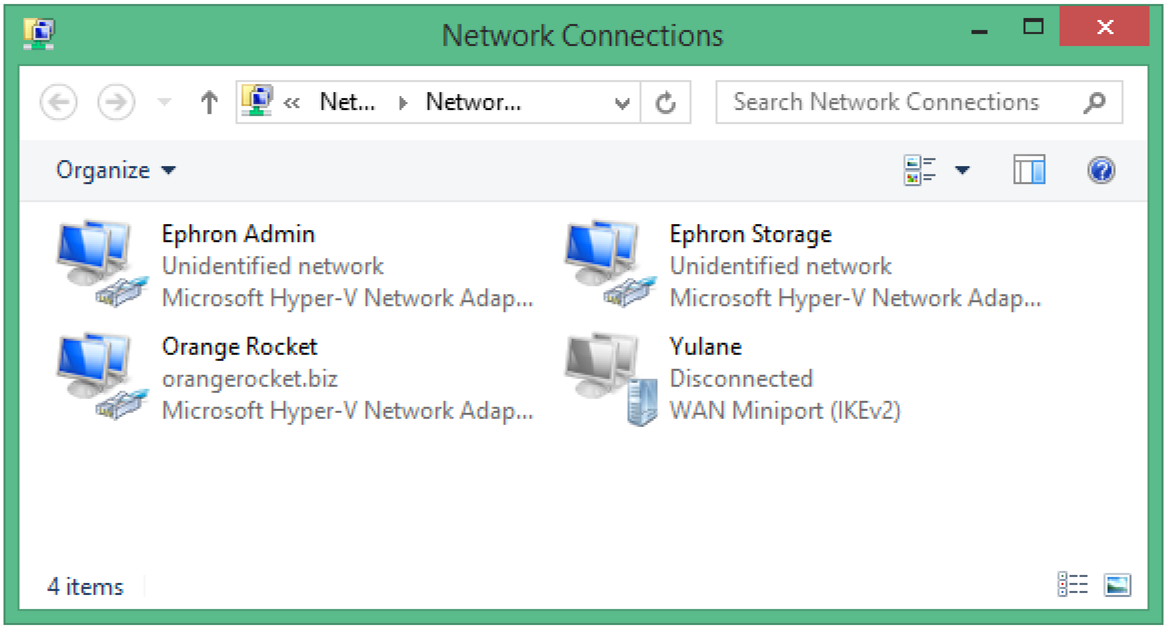
Destination name: Yulane

☐ Use a smart card

☑ Remember my credentials

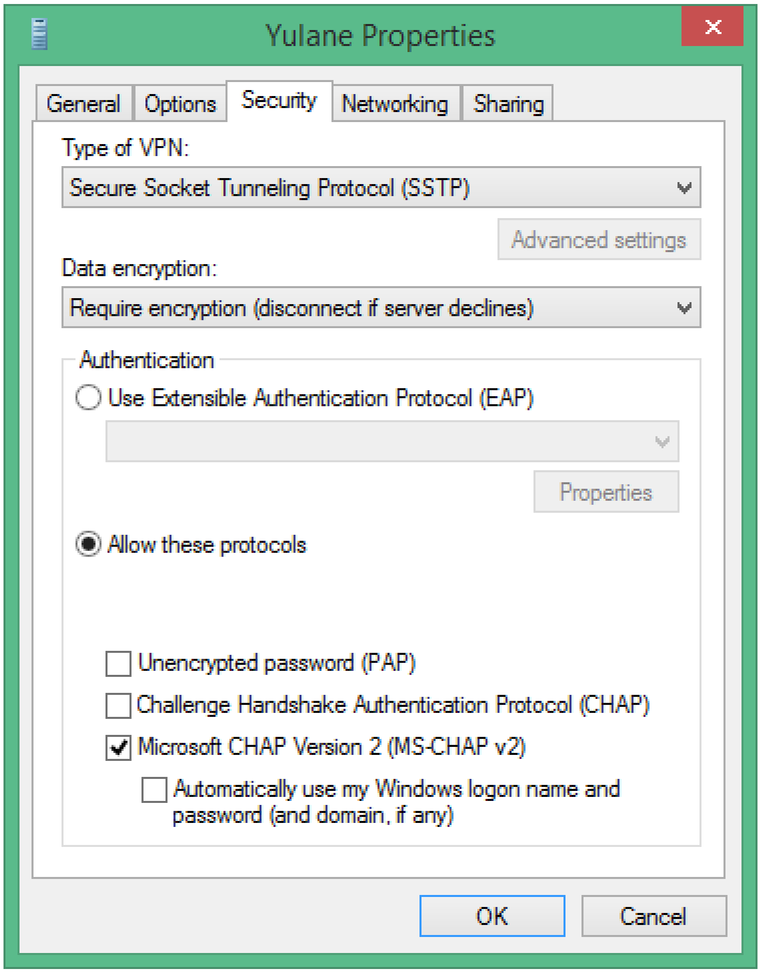
☑ Allow other people to use this connection
This option allows anyone with access to this computer to use this connection.

8. We now need to change the security settings. Go to Control Panel > Network and Internet > Network Connections.
9. Right click Yulane and select Properties



Ephron Admin Unidentified network Microsoft Hyper-V Network Adap...	Ephron Storage Unidentified network Microsoft Hyper-V Network Adap...
Orange Rocket orangerocket.biz Microsoft Hyper-V Network Adap...	Yulane Disconnected WAN Miniport (IKEv2)

10. Under the Security tab make the following changes:
    a. Type of VPN: Security Socket Tunneling Protocol (SSTP)
    b. Data encryption: Require encryption
    c. All these protocols: Microsoft CHAP Version 2 (Select Automatically use my Windows logon name and password if the machine has an active directory computer account)
11. Click Ok



Yulane Properties

Type of VPN:
Secure Socket Tunneling Protocol (SSTP)

Data encryption:
Require encryption (disconnect if server declines)

Authentication

○ Use Extensible Authentication Protocol (EAP)

● Allow these protocols

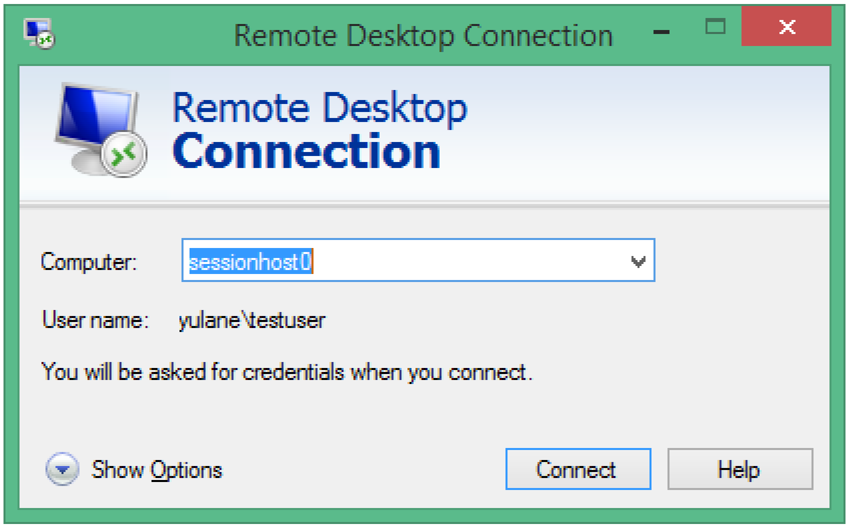
□ Unencrypted password (PAP)
□ Challenge Handshake Authentication Protocol (CHAP)
☑ Microsoft CHAP Version 2 (MS-CHAP v2)
□ Automatically use my Windows logon name and password (and domain, if any)

Virtual Desktop

Yulane staff may utilize the Yulane Remote Desktop Services remote virtual desktop referred to as SessionHost0. On it is Office 2016 Professional Plus, Visio 2016, Project 2016, and Acrobat XI Professional.

VPN

If connected using VPN then you may connect to SessionHost0 using the Remote Desktop Connection application. Since by virtual of being connected by VPN you are already in the network, no special settings are required to access the SessionHost0.



Computer: sessionhost0

User name: yulane\testuser

You will be asked for credentials when you connect.

RD Web

RD (Remote Desktop) Web is a web site that makes RemoteApp and SessionHost0 available simply by signing on to the site and clicking upon an icon. The user does not need to be connected by VPN to use this service. RemoteApp is a remote desktop version of a single application. The application runs and looks identical to the application were it running locally, but is actually running remotely.

When starting RemoteApp applications (Office 2016, Acrobat) or SessionHost0 Remote Desktop Connection the user will receive a number of warnings related to certificates. The user should accept all warnings.

Users must be in the Active Directory RD Users group in order to use RD Web.

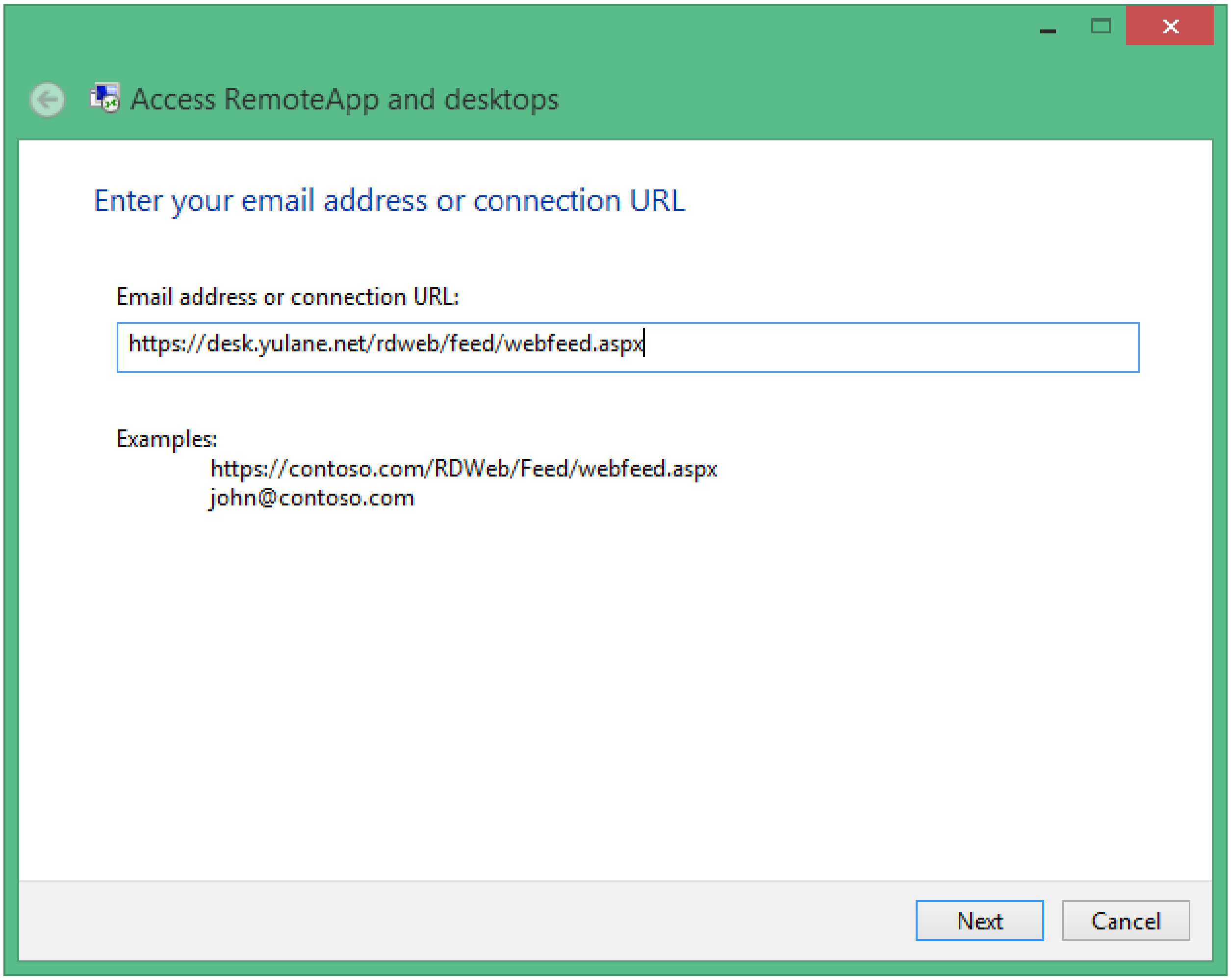
RD Web may require the use of Internet Explorer. FireFox and Chrome may not work properly.

To connect go to https://desk.yulane.net/rdweb

RemoteApp and Desktop Connections

RemoteApp and Desktop Connections is found in Windows 7, 8, and possibly 10. It integrates RDWeb into a person's personal computer. To setup, go to Control Panel > All Control Panel Items > RemoteApp and Desktop Connections and follow these instructions:

1. Click Access RemoteApp and desktops
2. Enter the URL https://desk.yulane.net/rdweb/feed/webfeed.aspx into the window
3. Click Next
4. Click Next



Enter your email address or connection URL

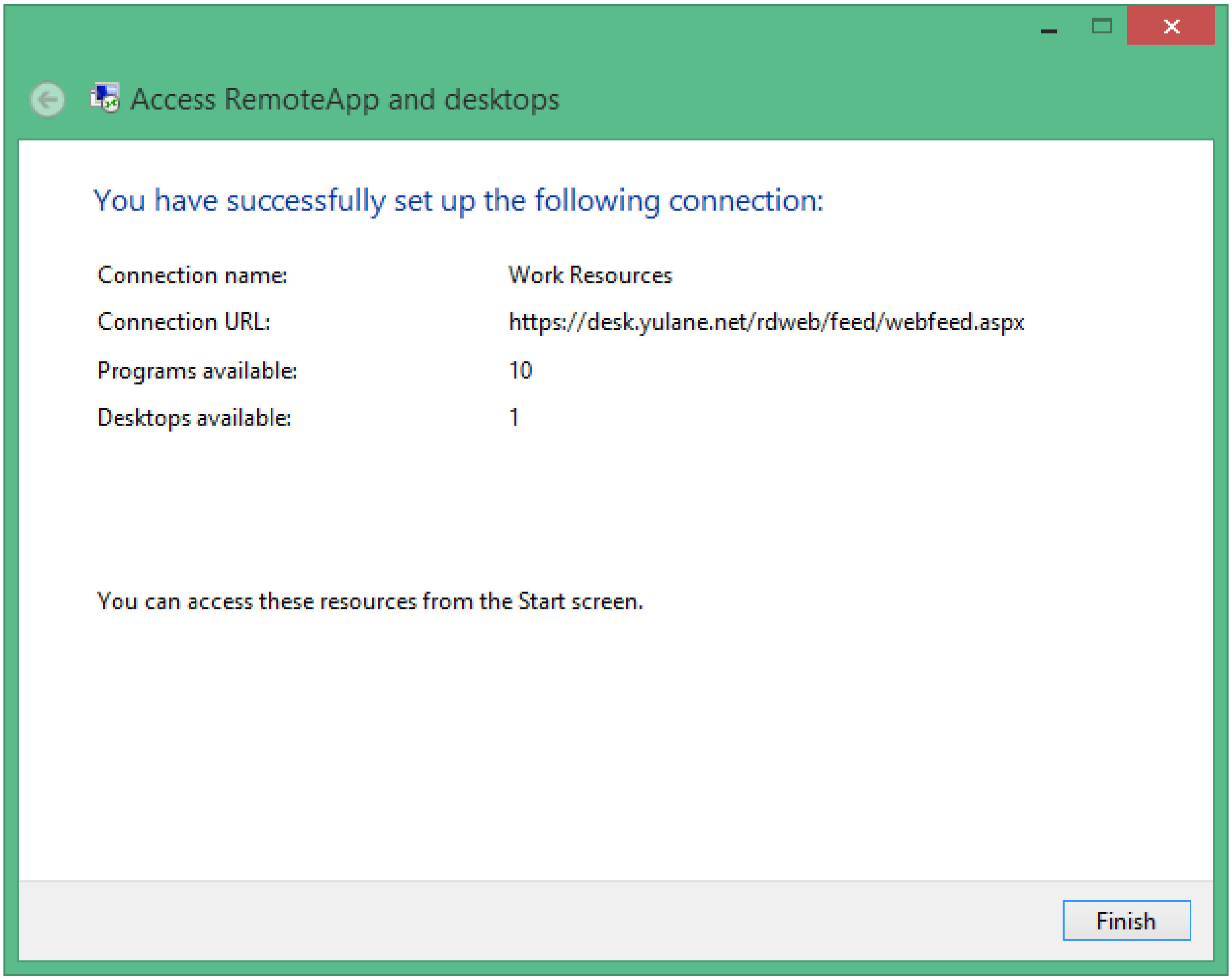
Email address or connection URL:

https://desk.yulane.net/rdweb/feed/webfeed.aspx

Examples:
https://contoso.com/RDWeb/Feed/webfeed.aspx
john@contoso.com

5. Supply your yulane credentials, such as yulane\testuser and password.

6. You will see the following when successful:



You have successfully set up the following connection:

Connection name: Work Resources

Connection URL: https://desk.yulane.net/rdweb/feed/webfeed.aspx

Programs available: 10

Desktops available: 1

You can access these resources from the Start screen.

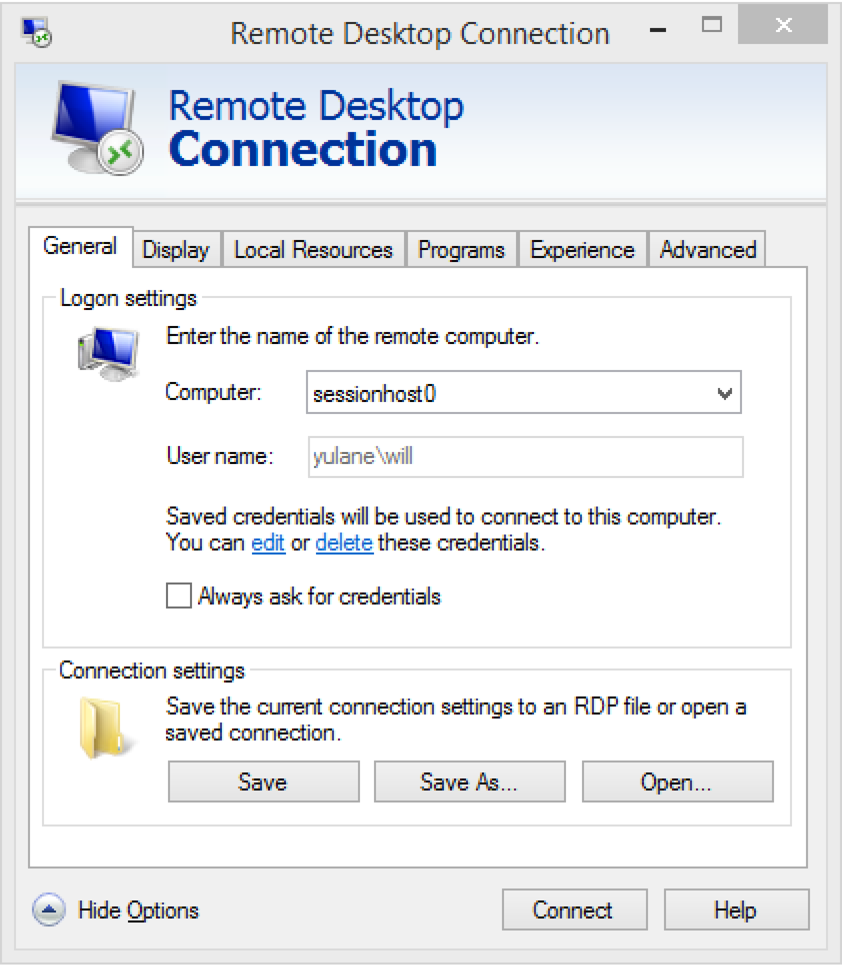
Notice that the Windows icon tray will have an icon for this service. All of the RemoteApp and remote (virtual) desktops will be accessible under Work Resources.

RD Gateway

RD Gateway is a service to allow users to connect to SessionHost0 without using RDWeb and without using VPN. Instead, the user just uses a simple Remote Desktop Connection. To do this, following these instructions in the Remote Desktop Connection application:

1. Under the General tab enter SessionHost0 under computer
2. Enter the username in the domain\user format
3. Optionally, uncheck *Always as for credentials*

4. Optionally click Save



Remote Desktop Connection

Remote Desktop Connection

Logon settings

Enter the name of the remote computer.

Computer: sessionhost0

User name: yulane\will

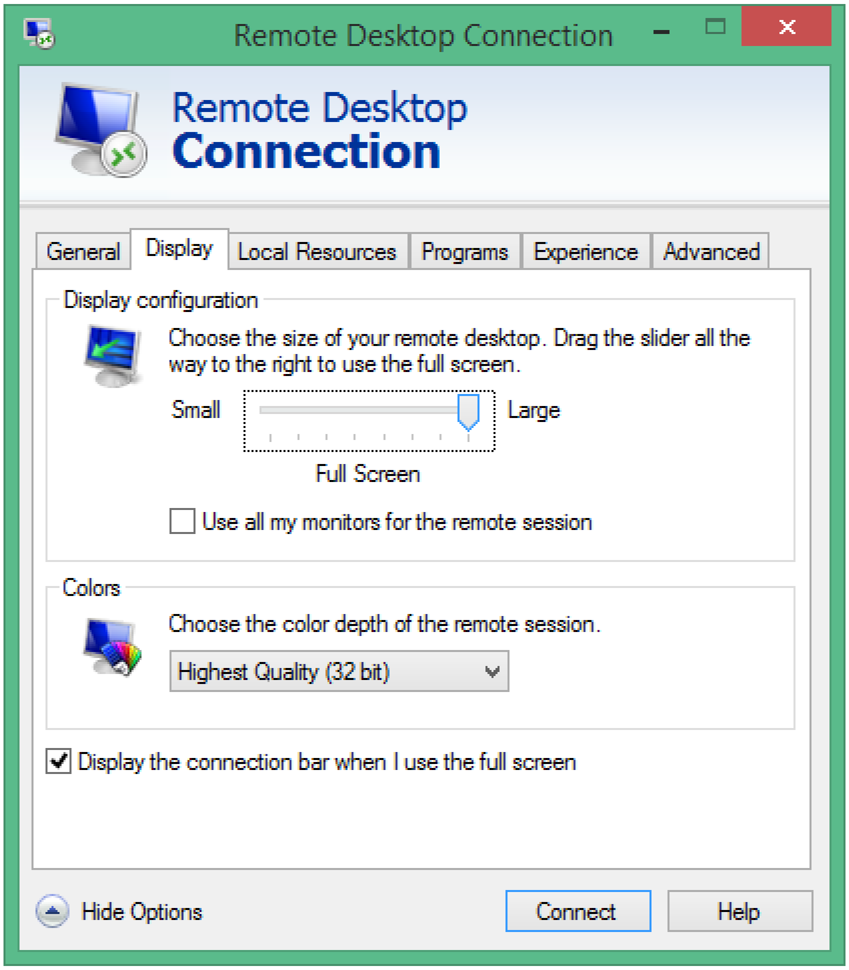
Saved credentials will be used to connect to this computer. You can edit or delete these credentials.

□ Always ask for credentials

Connection settings

Save the current connection settings to an RDP file or open a saved connection.

5. To connect using all of the screens on your computer select *Use all my monitors for the remote session.* To just use one screen, leave as below:



Display configuration

Choose the size of your remote desktop. Drag the slider all the way to the right to use the full screen.

Small — Large: Full Screen

□ Use all my monitors for the remote session

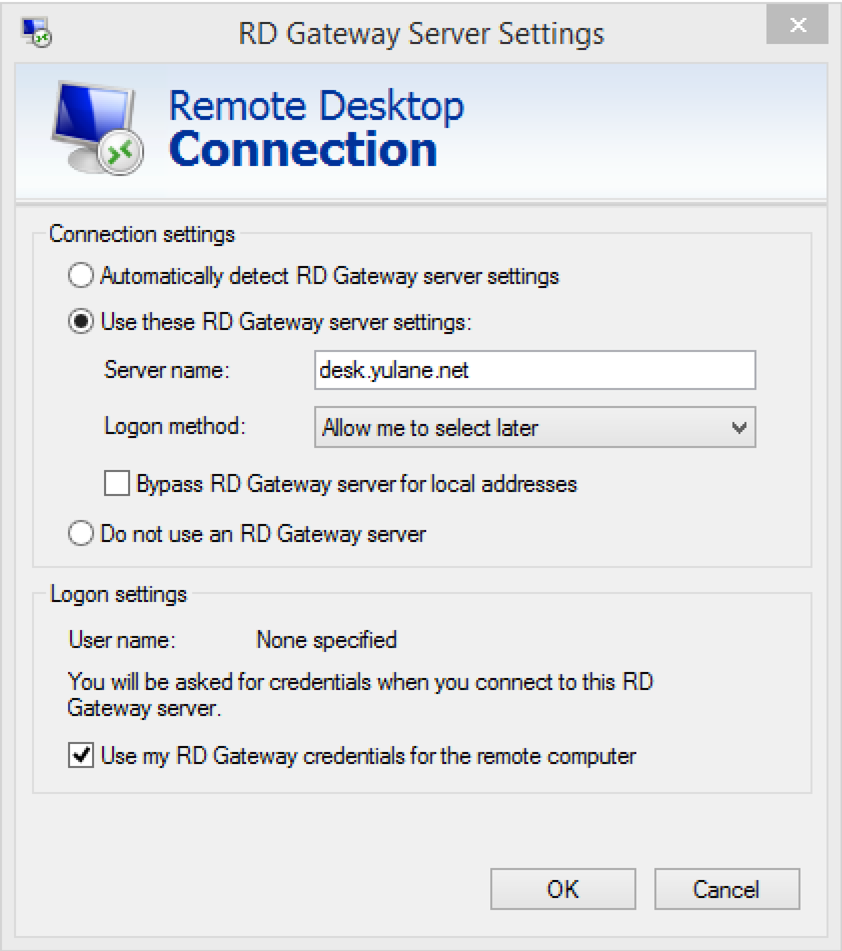
Colors

Choose the color depth of the remote session.

Highest Quality (32 bit)

☑ Display the connection bar when I use the full screen

6. On the Advanced tab click Settings
7. Select Use these RD Gateway server settings:
8. Enter desk.yulane.net
9. Select *Bypass RD Gateway server for local addresses*


RD Gateway Server Settings

Remote Desktop Connection

Connection settings

○ Automatically detect RD Gateway server settings

● Use these RD Gateway server settings:

Server name: desk.yulane.net

Logon method: Allow me to select later

□ Bypass RD Gateway server for local addresses

○ Do not use an RD Gateway server

Logon settings

User name: None specified

You will be asked for credentials when you connect to this RD Gateway server.

☑ Use my RD Gateway credentials for the remote computer

Be aware that if you set the RD Gateway settings in Remote Desktop Connection you may have to toggle the settings off (select Automatically detect RD Gateway server settings) and on if you are trying to sign into other computers not part of the Yulane network. Also, if Yulane adds an external DNS entry for sessionhost0.yulanet.net to point to desk.yulane.net then it may automatically connect without explicit settings.

Email

Yulane hosts email accounts under multiple domain names. It uses Microsoft Exchange 2016 as its mail server. Exchange is not engineered to handle multiple domain names for separate organizations, what is referred to as supporting *multi-tenancy*. So, while multiple domain names are supported, the structure of the system allows any user to use any domain name and for the system to support sending and receiving for any user on any domain name. There is no way to tell Exchange that it should only send and receive for a specific email domain name on a per user basis. However, Exchange can be told the default email address to use for a user.

Supporting multiple domains in a single AD domain pose additional problems. Amongst them is the configuration. If a user primarily uses abc.com as their domain and goes to setup that account, Exchange may want to setup the account as xyz.com since that is the name of the native active directory domain. It may expect connection and auto-discover settings to work on the native active directory domain and it may have no means to support configurations trying to use other domains. Further, connections are supposed to be made securely using an SSL certificate having a domain name the same as that defined by Exchange server for client connections. If the certificates common name does not match the connection destination a warning is given about names not matching.

Naturally, an environment supporting multiple domain names cannot support multiple users with the same name since Exchange tightly integrates with active directory and only a single username is allowed in it. Microsoft has written a number of white papers describing how multi-tenancy might work and thus supporting high density multiple organization hosting on a single deployment of Exchange, but it is far from easy to get this right and keep organizations properly separated from each other.

In regards to the Yulane deployment, a user having used the wecare.yulane.net configuration will still be able to use their UsChinaEscrow.com email normally. All domain names point to the same place. Exchange has a standard policy for all new users related to their Default Reply-To email address. It is wecare.yulane.com. However, each user can be individually customized by unchecking the *Apply default policy* setting and one of the supported Receive domain names applied as the new default, which is actively performed currently.

Outlook 2016 Profile Recreation

If the Exchange configuration is no longer valid and needs to be reset, this normally occurs by closing Outlook, going to Control Panel > Mail, deleting the mail profile, opening Outlook and allowing auto-discover to create new settings. However, Outlook in Windows Server 2012 R2 does not support this technique. Therefore, the profile must be deleted using the registry. Perform this task as follows:

1. Close Outlook
2. Open Windows Run or the Command Line and type regedit to open the Windows registry editor

Navigate to HKEY_CURRENT_USER\Software\Microsoft\Office\15.0\Outlook\Profiles

3. Delete any folders below Profiles
4. Open Outlook and allow it to setup your account

Connecting to Exchange using ActiveSync

While ActiveSync has been around for a long time to support mobile devices, in the desktop version of Outlook 2016 for the first time supports ActiveSync as its primary *external* Exchange access technique. Therefore, ActiveSync will continue to support mobile devices and the desktop version of Outlook starting in version 2016.

When connected to the network with VPN or inside of the network, such as through SessionHost0 or a VPN or DirectAccess connected computer having an account in active directory, Outlook discovers its settings automatically and the protocol used is MAPI. In all other circumstances, such as on mobile devices or external computers not connected directly to the network or using VPN, ActiveSync is used.

Connecting via Outlook 2016 to Exchange server using ActiveSync has not yet been successful despite Microsoft's Connectivity Analyzer stating that the Exchange server's ActiveSync is working normally, efforts to utilize the service have failed and continue to be explored.

Connecting to Outlook Anywhere (Outlook 2013 or earlier Only)

Outlook Anyway was a technology that supported RPC over HTTP. The result was that a person could use Outlook with an Exchange server account within being physically in the network or connected using VPN. The technology was eliminated in Outlook 2016 in favor of ActiveSync, which is the mobile Outlook support technology. The procedure for using Outlook Anywhere follows:

1. Go to Windows Control Panel
2. Search for *Mail*
3. Open Mail
4. Click *Show Profiles…*
5. Click *Add…*
6. Type *Yulane*
7. Click *Ok*
8. The Add Account dialog box will display
9. Select *Manual setup...*
10. Click *Next*
11. Click *Nex*
12. Type Server: *wecare.yulane.com*
13. Type User Name: *<your username>*
14. Click *More Settings...*
15. Click *Connection* tab
16. Select *Connect to Microsoft Exchange...*
17. Click *Exchange Proxy Settings...*
18. for https:// type *wecare.yulane.com*
19. Select *Only connect to proxy servers....*
20. type *msstd:wecare.yulane.com*
21. Click *Ok*
22. Click *Ok*
23. Click *Next*

Links in Emails Are Disabled

By default, Outlook disables links in email as a security precaution so that users do not download malicious software. To disable this capability read this Office help document: https://support.office.com/en-us/article/Turn-on-or-off-links-in-email-messages-2d79b907-93b6-4774-82e6-1f0385cf20f8

Full Access and *Send As* Permissions

Exchange and Outlook support two capabilities named Full Access and Send As permissions. Full Access grants one user full access to an email account other than their own. *Send As* provides permissions to send emails on behalf of another user in which a mailbox exists.

Full Access and Send As permissions are enabled and disabled through the Exchange Console. Setting Send As permissions may fail if the active directory user is not inheriting permissions from the OU in which it resides. However, in cases where the user's security is updated to inherit and the problem persists it is possible to set Send As in the active directory security settings on the user. Exchange

Console appears to merely be adding a role to the user’s permissions named Send As that merely needs to be checked to work.

Network File System and Permissions

Yulane has a network file system that is accessible through a number of network shares. These are accessed using an UNC path that always starts with \\Store. These files and folders can be accessed like a user would access any file on their local file system.

Yulane controls access to the network file system with two active directory security groups. These are Staff and Owners. Neither of these groups are related to SharePoint and are exclusive to the active directory system and currently only relevant to network file system permissions. The Owners group has full control of all files within the network file system. The Staff group only has access to the File Store directory.

SharePoint Access Control

While access control within SharePoint is applied to active directory user accounts, the actual permissions enforcement occurs only in SharePoint. Therefore, no permissions changes for SharePoint should occur within Active Directory. User access control for SharePoint should be managed exclusively within SharePoint access control interfaces.

Users

New User Setup

Yulane managers will manage SharePoint access control for any new users. Before this can be done, the following information must be supplied so that the user can obtain an active directory account, have their network access defined, and have an email account established. For this to be done, the following is needed:

- Name
- Sign on and mailbox account name (username)
- Password (not recommended for passwords to be stored in plain text as they currently are)
- Whether the user should have Virtual Desktop/RemoteApp access (membership in RD Users security group)
- Whether the user should have VPN access (members in VPN User security group)
- Whether the user is in the Owners security group for network file system access or in the Staff security group for access only to the File Folder shared directory

Managing Inactive Users

For security reasons, it is recommended that when a user leaves the organization that their password be reset and the user be disabled in active directory, but that the user not be deleted. This ensures the user cannot gain access to the system, delete emails, or delete files on the network file system out of anger. Currently, Yulane has a considerable number of such users who, if they wanted, could delete some aspects of the system, namely their own mailboxes or possible entries in SharePoint.

Disabling access to a user no longer with the organization blocks their ability to gain access, but does not permanently remove access to their data. After a user has left mailbox access can be granted to staff my setting Full Access permissions in Exchange even if the active directory user is disabled from signing on.