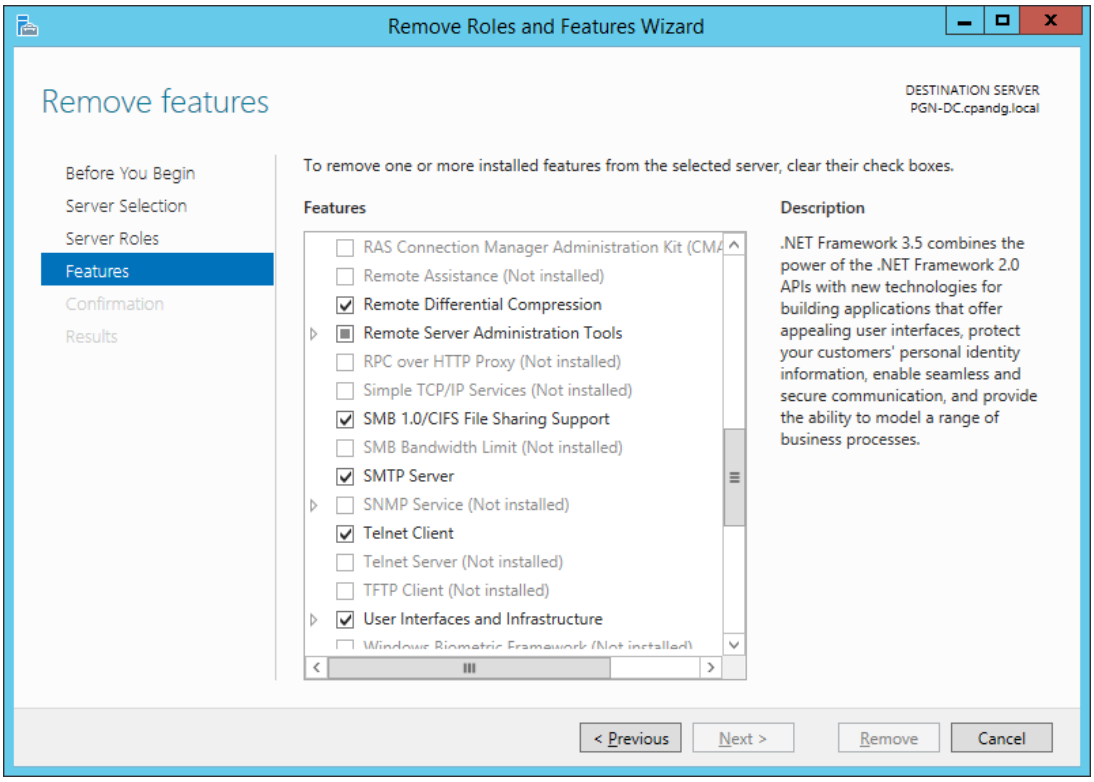
D&S Helpdesk

On-prem Windows Server SMTP Relay Services and Office 365

Mark T of D&S - 2022-01-27 - 0 Comments - in Office 365

Now that D&S is migrating more clients' email services to the cloud, we're losing the on-premises SMTP services from Exchange Server and/or MDaemon. In addition to the mailboxes that were being hosted, these applications could also be used to relay system alerts using SMTP. The problem is these applications are licensed, and it isn't practical to keep paying for them just to maintain alerting when there is a free & simpler Windows feature to accomplish this task - **SMTP Server**.



There is some pre-requisite work before you can start using these SMTP services. Firstly, you need a public FQDN that corresponds to the client's external IP address. It doesn't necessarily have to be a static IP address either - but there will be some limitations and additional configuration steps required later if there isn't.

I - **If the client has a static IP address**, we can assume they also have a registered domain for which we can create DNS A-Records for the static IP addresses. In the case of PGN, there are 2 'mail.kwaccountants.ca' A-records - one for each of their static IPs. Using 'NSLOOKUP' from a command prompt:

> mail.kwaccountants.ca

Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: mail.kwaccountants.ca
Addresses: 69.165.165.111
          72.143.35.138

II - **If the client has a dynamic IP address** and has a Peplink router managed through InControl2 (under warranty), Peplink provides a free, public hostname with a 'mypep.link' extension that automatically updates with the router's public IP address(es). If the router isn't a Peplink under warranty, 95% of the routers out there come with a dynamic DNS client that can be configured to connect to a number of free dynamic DNS providers out there like No-IP or DynDNS. Harlock-Schultz has a dynamic IP address:

> hs-soho.mypep.link
Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
Name: hs-soho.mypep.link
Address: 206.248.171.79

Using the client's FQDN, update their DNS SPF (TXT) record to include this hostname. The **SPF record identifies sources authorized to send email** on behalf of the associated domain - not to be confused with an **MX record, which advertises the hosts authorized to receive email** for the associated domain. For example, here are the MX records for harlockschultz.com and kwaccountants.ca:

> set type=mx

> harlockschultz.com

Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
harlockschultz.com   MX preference = 0, mail exchanger = harlockschultz-com.mail.protection.outlook.com

> kwaccountants.ca

Server: dns.google
Address: 8.8.8.8

Non-authoritative answer:
kwaccountants.ca   MX preference = 0, mail exchanger = kwaccountants-ca.mail.protection.outlook.com

This indicates the mailboxes for these respective domains are in the Office 365 cloud, **so**

that's where email is received.

> set type=TXT

> harlockschultz.com
Server: dns.google
Address: 8.8.8.8

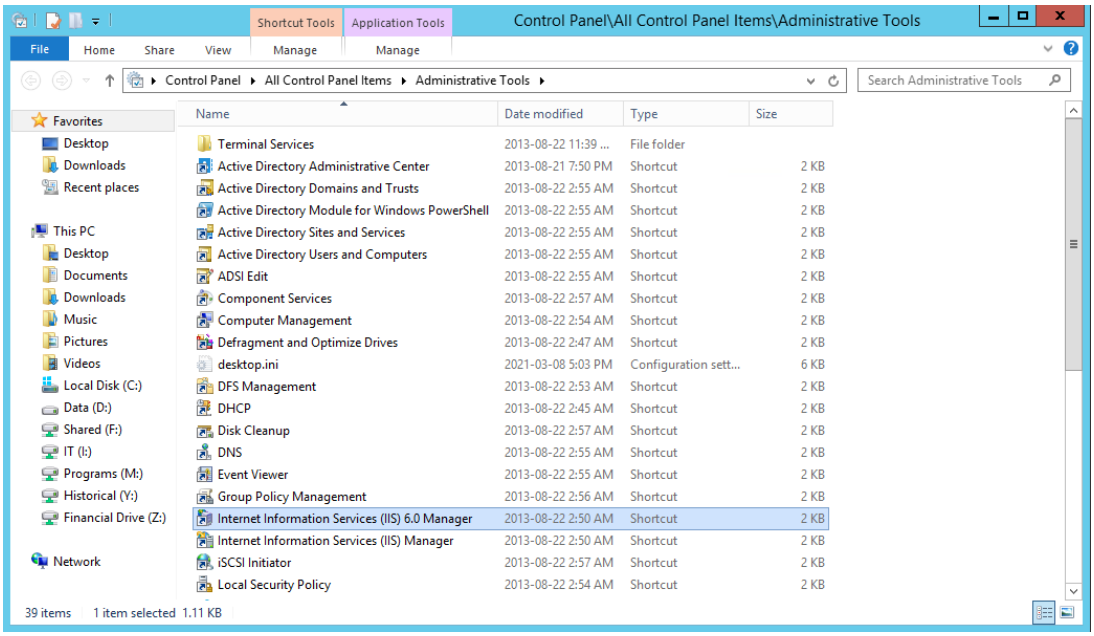
Non-authoritative answer:
harlockschultz.com text = "v=spf1 include:spf.protection.outlook.com a:hs-soho.mypep.link -all"

> kwaccountants.ca
Server: dns.google
Address: 8.8.8.8

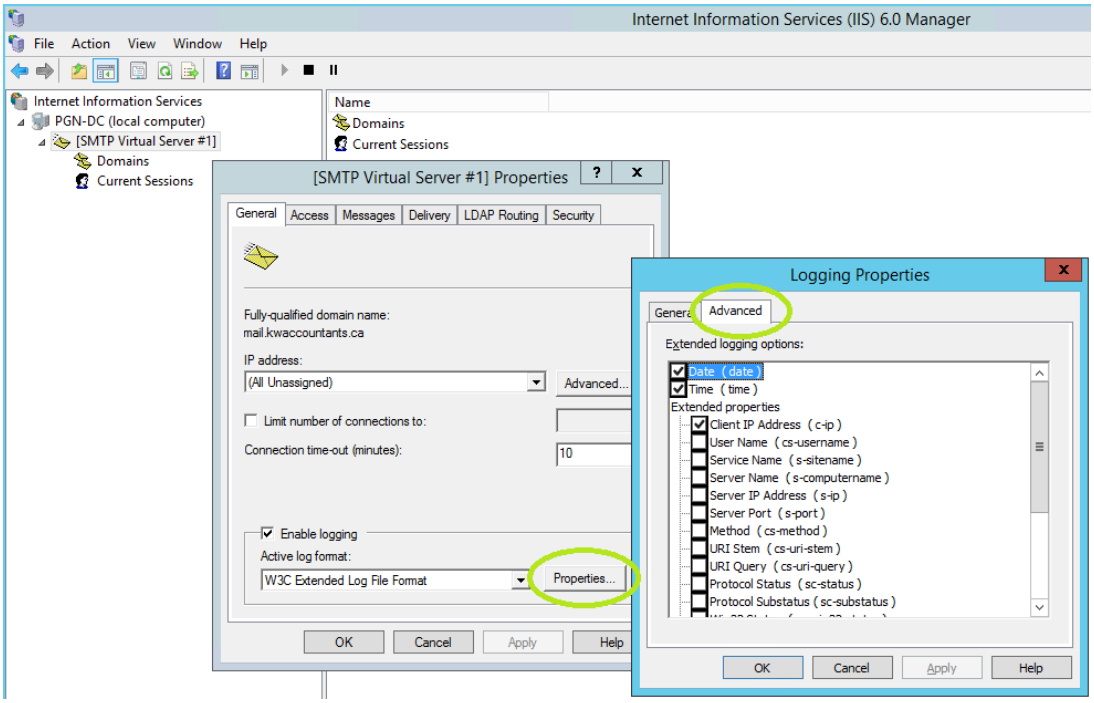
Non-authoritative answer:
kwaccountants.ca text = "v=spf1 mx a:mail.kwaccountants.ca include:spf.protection.outlook.com -all"

This indicates a Microsoft-managed list (spf.protection.outlook.com) for both domains with the hosts and IP addresses authorized for **sending email**. Notice the 'a:<FQDN>' entries in the text records - these hostnames are also authorized to **send email for the domain**.

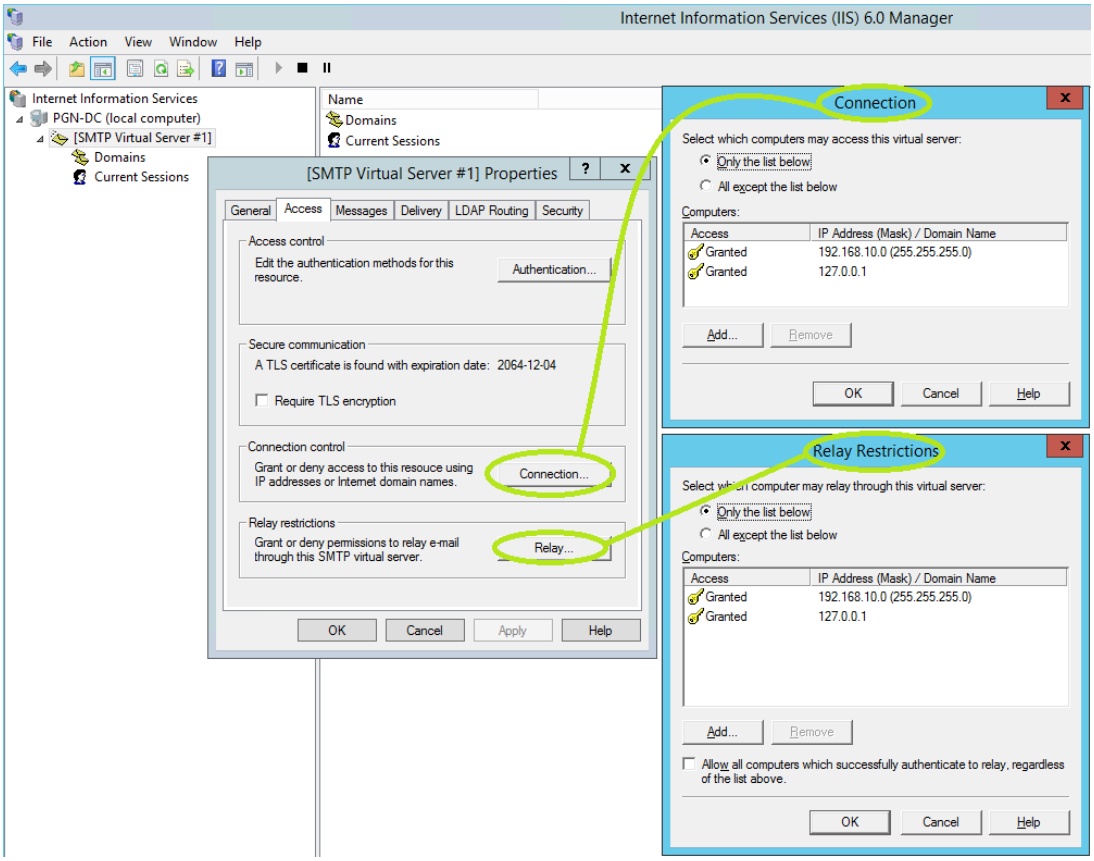
With the A-record(s) and TXT-record in place, we can proceed with the SMTP Server setup. After SMTP Server has been installed, the management tool for it is '**Internet Information Services (IIS) 6.0 Manager**' in 'Administrative Tools':



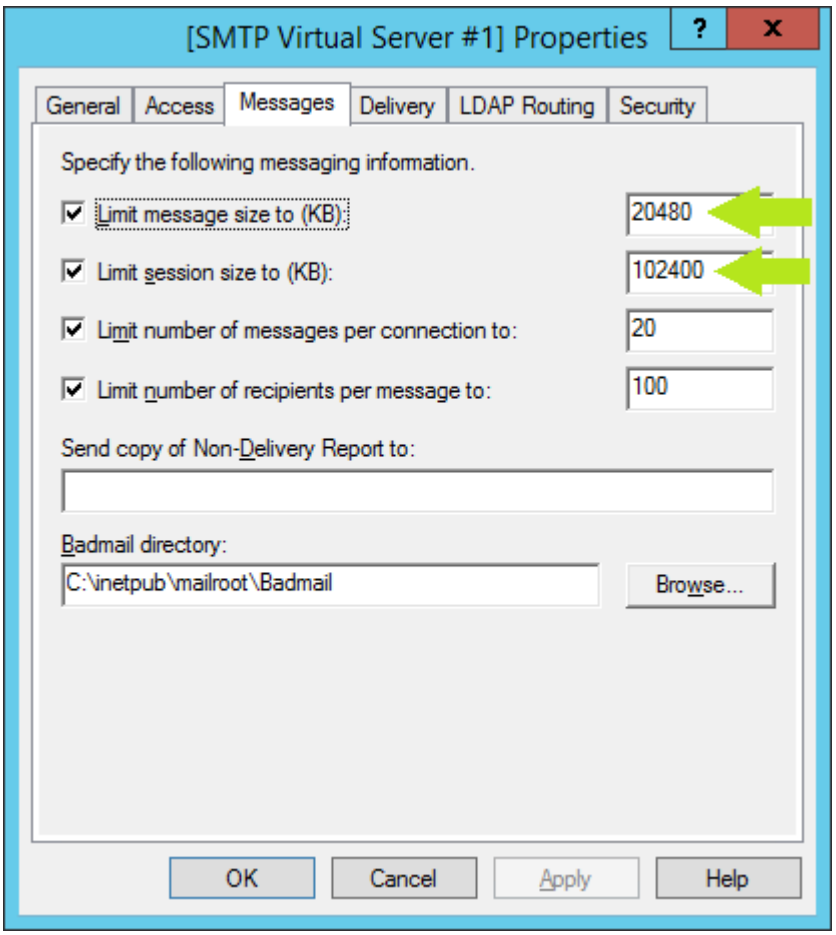
Logging enabled, make sure date/time and client IP address are selected options...



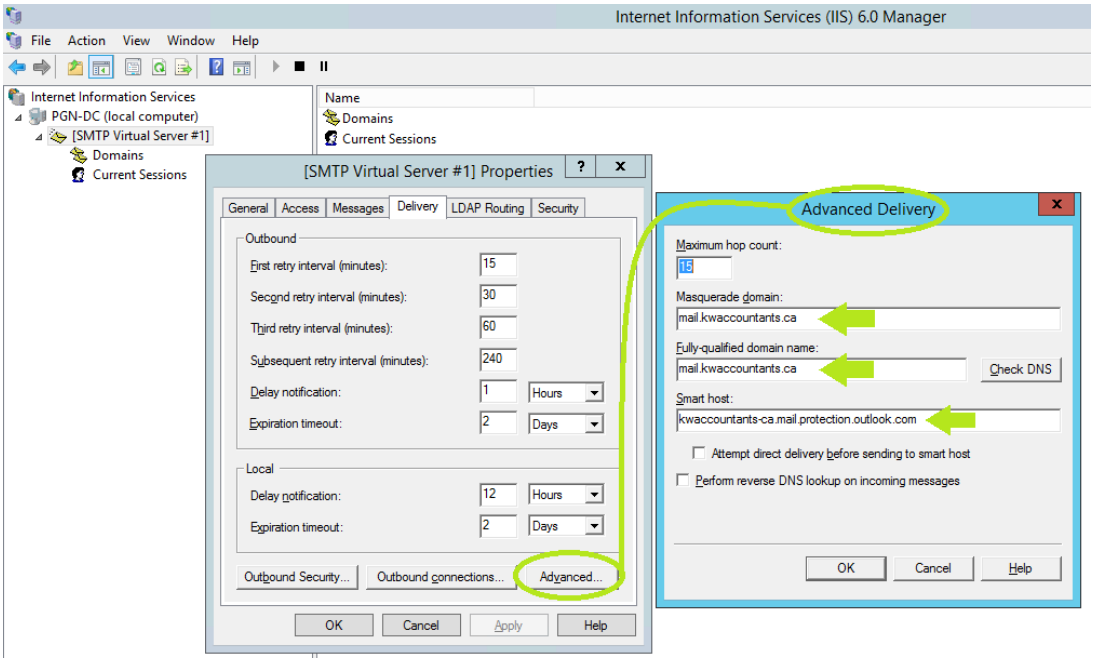
Secure the server by restricting connections to the LAN or itself (loopback)...



The default message limits may be too small, particularly if the service may be used by office scanners. I just added a '0' to the end of the 2 values indicated below...



Set the 'Masquerade domain' and the 'Fully-qualified domain name' to the DNS A-record you created for resolving the client's public IP address. The 'Smart host' value is the same as the MX-record for the domain...



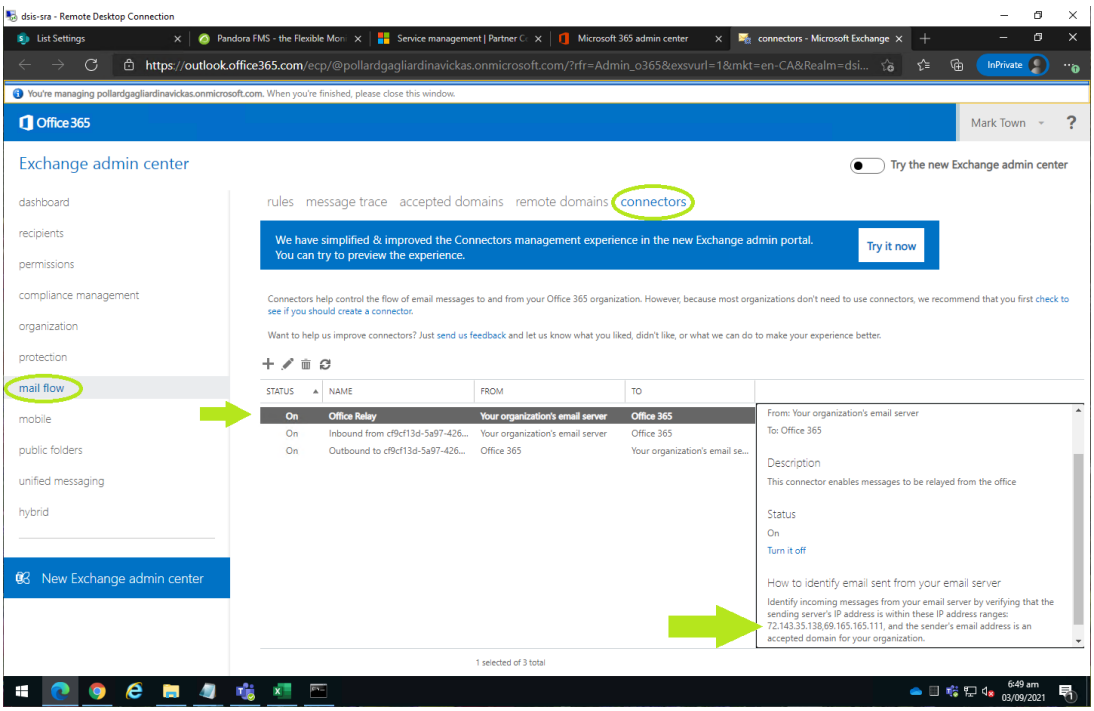
Also, check 'Outbound Security' and **ensure 'TLS encryption' has a checkmark**.

The SMTP relay server is ready for use. Point the client (PowerChute notification, office

scanner) to the server's internal IP address, or the internal hostname; select a sender email address from the domain (doesn't need to exist) like PowerChute@KWAccountants.ca, but the recipient email, at this point, is limited to an actual mailbox or distribution list on the same domain. PowerChute@KWAccountants.ca can send to Administrator@KWAccountants.ca, but not to HelpDesk@DSInfinITe.Solutions.

This takes us back to whether or not the client has a static IP address.

I - **If the client has a static IP address**, then you need to create a **Receive Connector** in Exchange Admin (Office 365) to confirm any email received from the specific IP addresses should be trusted. With this enabled, the internal client can specify ANY email address for a recipient, and it will be relayed (and trusted) coming from Office 365:



II - If the client does not have a static IP address, the only way to get an email notification to helpdesk@dsinfinite.solutions requires 2 steps:

a) Add 'helpdesk@dsinfinite.solutions' as a Global address book contact using Exchange Admin
b) create a 'DSInfinITe@harlockschultz.com' (for example) distribution group, and add the 'helpdesk@dsinfinite.solutions' contact as a member of the group. Set PowerChute or MEGARAID to email alerts to 'DSInfinITe@harlockschultz.com', and it will be relayed to our helpdesk.