D&S Helpdesk

Portal > Knowledgebase > Office 365 > On-prem Windows Server SMTP Relay Services and Office 365

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 onpremises 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**.

Ē.	Remove Roles and Features Wizard	_ _ X				
Remove features Before You Begin	To remove one or more installed features from the selected sen	DESTINATION SERVER PGN-DC.cpandg.local ver, clear their check boxes.				
Server Selection	Features	Description				
Server Roles	RAS Connection Manager Administration Kit (CMA	.NET Framework 3.5 combines the				
Features	Remote Assistance (Not installed)	APIs with new technologies for				
Confirmation	Remote Differential Compression	building applications that offer				
Results	Remote Server Administration Tools	appealing user interfaces, protect				
	RPC over HTTP Proxy (Not installed)	information, enable seamless and				
	Simple TCP/IP Services (Not installed)	information, enable seamless and secure communication, and provide				
	SMB 1.0/CIFS File Sharing Support	the ability to model a range of business processes.				
	SMB Bandwidth Limit (Not installed)					
	SMTP Server					
	SNMP Service (Not installed)					
	✓ Telnet Client					
	leinet Server (Not installed)					
	IFIP Client (Not installed)					
	User Interfaces and Infrastructure					
< Previous Next > Remove Cancel						

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

> <u>harlockschultz.com</u>

Server: dns.google Address: 8.8.8.8

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

> kwaccountants.ca

Server: dns.google Address: 8.8.8.8

Non-authoritative answer: kwaccountants.ca MX preference = 0, mail exchanger = kwaccountantsca.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

> <u>harlockschultz.com</u>

Server: dns.google Address: 8.8.8.8

Non-authoritative answer: harlockschultz.com text = "v=spf1 include:spf.protection.outlook.com a:hssoho.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':

🖄 l 🔂 🔝 🗢 l		Shortcut Tools	Application Tools		Control Panel\A	II Control Panel Ite	ems\Administra	ative Tools		x	
File Home Share	View	Manage	Manage							~ (9
(j) (i) (i) (i) (i) (i) (i) (i) (i) (i) (i	🕞 🗇 🕆 🔞 > Control Panel > All Control Panel Items > Administrative Tools > 🗸 🖒 Search Administrative Tools >]			
							Γ	-			
🔆 Favorites	Name				Date modified	Туре	Size			- 1	
Desktop	퉬 Term	inal Services			2013-08-22 11:39	File folder					
🚺 Downloads	🛃 Activ	e Directory Admir	istrative Center		2013-08-21 7:50 PM	Shortcut	2 KB				
🔛 Recent places	📷 Activ	e Directory Domai	ins and Trusts		2013-08-22 2:55 AM	Shortcut	2 KB				
	🔝 Activ	e Directory Modul	e for Windows Powe	rShell	2013-08-22 2:55 AM	Shortcut	2 KB				
🌉 This PC	💦 Activ	e Directory Sites a	nd Services		2013-08-22 2:55 AM	Shortcut	2 KB				
隆 Desktop	🖲 Activ	e Directory Users a	and Computers		2013-08-22 2:55 AM	Shortcut	2 KB				-
Documents	💦 ADSI	Edit			2013-08-22 2:55 AM	Shortcut	2 KB				
🐌 Downloads	휁 Com	ponent Services			2013-08-22 2:57 AM	Shortcut	2 KB				
🚺 Music	🛃 Com	puter Managemer	nt		2013-08-22 2:54 AM	Shortcut	2 KB				
📔 Pictures	🐞 Defra	gment and Optim	ize Drives		2013-08-22 2:47 AM	Shortcut	2 KB				
📔 Videos	🗿 deskt	op.ini			2021-03-08 5:03 PM	Configuration sett	6 KB				
🃥 Local Disk (C:)	💏 DFS N	/lanagement			2013-08-22 2:53 AM	Shortcut	2 KB				
👝 Data (D:)	混 DHCF	b			2013-08-22 2:45 AM	Shortcut	2 KB				
🖵 Shared (F:)	震 Disk (Cleanup			2013-08-22 2:57 AM	Shortcut	2 KB				
🖵 IT (l:)	🚴 DNS				2013-08-22 2:55 AM	Shortcut	2 KB				
🖵 Programs (M:)	🔝 Event	Viewer			2013-08-22 2:55 AM	Shortcut	2 KB				
🖵 Historical (Y:)	😹 Group	Policy Managen	nent		2013-08-22 2:56 AM	Shortcut	2 KB				
🖵 Financial Drive (Z:)	뉡 Intern	net Information Se	rvices (IIS) 6.0 Manag	ger	2013-08-22 2:50 AM	Shortcut	2 KB				
	濻 Intern	net Information Se	rvices (IIS) Manager		2013-08-22 2:50 AM	Shortcut	2 KB				
👊 Network	🔝 iscsi	Initiator			2013-08-22 2:57 AM	Shortcut	2 KB				
	🛃 Local	Security Policy			2013-08-22 2:54 AM	Shortcut	2 KB			-	~
39 items 1 item selected	39 items 1 item selected 1.11 KB										

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

👣 Inte 👣 File Action View Window Help	ernet Information Services (IIS) 6.0 Manager
👣 File Action View Window Help	
🗢 🏟 🙍 📰 🗟 😖 🛛 🎫 🕨	
Internet Information Services Internet Sessions Internet Session	Logging Properties X General Advanced Extended logging options: Image: State of the state of th
OK Cancel Apply Help	OK Cancel Apply Help

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

G.	Internet Information Services (IIS) 6.0 Manager			
🕥 File Action View Window Help				
(≠ ⇒) 2 📷 🗟 Q 📄 🛛 🖬 🕨 🗉				
Internet Information Services	Connection			
△ [SMTP Virtual Server #1]	Select which computers may access this virtual server:			
Current Sessions [SMTP Virtual Se	erver #1] Properties ? X C All except the list below			
General Access Messages Deliv	very LDAP Routing Security Computers:			
Access control	Access IP Address (Mask) / Domain Name			
Edit the authentication methods freesource.	or this Authentication			
Secure communication	Add Remove			
Require TLS encryption	OK Cancel Help			
Connection control	Relay Restrictions ×			
IP addresses or Internet domain r	Select which computer may relay through this virtual server:			
Relay restrictions	Control the list below:			
Grant or deny permissions to relay through this SMTP virtual server	y e-mail Relay Computers:			
	Access IP Address (Mask) / Domain Name			
	Granted 192.168.10.0 (255.255.255.0)			
OK Car	ncel Apply Help of Granted 127.0.0.1			
	Add			
	Allow all computers which successfully authenticate to relay, regardless of the list above.			
	OK Cancel Help			

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...

[SMTP Virtual Server #1] Propert	ies ? X		
General Access Messages Delivery LDAP Routing	Security		
Specify the following messaging information.			
☑ Limit message size to (KB):	20480		
Limit session size to (KB):	102400		
☑ Limit number of messages per connection to:	20		
☑ Limit number of recipients per message to:	100		
Send copy of Non- <u>D</u> elivery Report to:			
Badmail directory:			
C:\inetpub\mailroot\Badmail	Browse		
OK Cancel Apply	Help		

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...

9	Internet Information Services (IIS) 6.0 Manager				
🐚 File Action View Window H	Help				
🗢 🄿 🙍 🔜 🖬 🖬 🖬					
Internet Information Services PON-DC (local computer) Some Services (SMTP Virtual Server #1) Somains Current Sessions G	Name Domains C Current Sessions [SMTP Virtual Server #1] Properties Properties Polyperties	Advanced Delivery X			
	Erist retry interval (minutes): 15 Second retry interval (minutes): 30 Tigird retry interval (minutes): 60 Subsequent retry interval (minutes): 60 Subsequent retry interval (minutes): 240 Delay notification: 1 Expiration timeout: 2 Delay notification: 12 Hours Outbound Security Outbound gonnections Ok Cancel Apply Help	Image: The second se			

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 <u>PowerChute@KWAccountants.ca</u>, but the recipient email, at this point, is limited to an actual mailbox or distribution list on the same domain. <u>PowerChute@KWAccountants.ca</u> can send to <u>Administrator@KWAccountants.ca</u>, but not to <u>HelpDesk@DSInfinITe.Solutions</u>.

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:

😼 dsis-sra - Remote Desktop Connection				– Ø ×
회 List Settings 🛛 🗙 🧔 Pandora	ra FMS - the Flexible Moni 🗙 🛛 💾 Service managemen	nt Partner Ge 🗙 📔 Microsoft :	365 admin center 🛛 🗙 🏹	connectors - Microsoft Exchange x $+$ - $ \boxdot $ X
\leftarrow $ ightarrow$ $m{C}$ $m{D}$ https://outlook.offic	ice365.com/ecp/@pollardgagliardinavickas.			=en-CA&Realm=dsi 🏠 🖆 庙 🚺 👘
You're managing pollardgagliardinavickas.onmicrosoft.c	com. When you're finished, please close this window.			
Coffice 365				Mark Town 👻 ?
Exchange admin center				Try the new Exchange admin center
dashboard	rules message trace accepted dor	mains remote domains	connectors	
recipients	We have simplified & improved the Con You can try to preview the experience.	nectors management experie	ence in the new Exchange a	dmin portal. Try it now
permissions				
compliance management	Connectors help control the flow of email messages see if you should create a connector.	to and from your Office 365 organiz	ation. However, because most org	anizations don't need to use connectors, we recommend that you first \ensuremath{check} to
organization	Want to help us improve connectors? Just send us fe	eedback and let us know what you lik	ked, didn't like, or what we can do	to make your experience better.
protection	+ / 亩 2			
mail flow	STATUS A NAME	FROM	то	
mobile	On Office Relay On Inbound from cf9cf13d-5a97-426	Your organization's email server Your organization's email server	Office 365 Office 365	From: Your organization's email server To: Office 365
public folders	On Outbound to cf9cf13d-5a97-426	Office 365	Your organization's email se	Description
unified messaging				This connector enables messages to be relayed from the office
hybrid				Status
				On Turn it off
🕼 New Exchange admin center				How to identify email sent from your email server
				Identify incoming messages from your email server by verifying that the sending server's IP address is within these IP address ranges: 72:143.35:138.69.165.165.111, and the sender's email address is an accepted domain for your organization.
		1 selected of 3 total		
🗯 💽 🥥 😂 🔚 🥥 🧃	🐮 💶 🔤			■ ■ 🤹 駅 4 👷 649 am 03/09/2021 🖣

II - If the client does not have a static IP address, the only way to get an email notification to <u>helpdesk@dsinfinite.solutions</u> 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.