# 

### **10ZiG MANAGER SECURE CONNECTOR**

### INSTALLATION GUIDE FOR REMOTE CLIENTS



Version: 1.0

Document Reference: TZMCC0001



Date: September 2020

Great care has been taken to ensure that the information contained in this document is accurate and complete. Should any errors or omissions be discovered, or should any user wish to suggest improving this document, they are invited to send the relevant details to:

**10ZiG Technology** 

North America (Rest of the world): info@10zig.com

EMEA: info@10zig.eu

© 10ZiG Technology

All rights are reserved. Reproduction in whole or in part is prohibited without the written consent of the copyright owner. All brand names and product names in this document are trademarks or registered trademarks of their respective companies.

### 10 ZiG.

### DISCLAIMER

10ZiG Technology reserves the right to revise or make changes or improvements to the products described in this document or to the document itself at any time without obligation to notify any person of such revision or improvements.

### **DOCUMENT VERSION CONTROL AND REVIEW HISTORY**

#### **Document Version Control**

Version	Created by	Date	Authorised & Checked
1.0	S.Hayles	18/09/2020	K.Greenway

### **REVIEW HISTORY**

September 2020

Creation of this document

### **CONTENTS**

DISCLAIMER	3	
DOCUMENT VERSION CONTROL AND REVIEW HISTORY	4	
REVIEW HISTORY		
CONTENTS	;	
LIST OF FIGURES	6	
OVERVIEW	7	
DEPLOYMENT SCENARIO 1 CONFIGURATION GUIDE	10	
MANAGER INSTALLATION AND CONFIGURATION	11	
MANAGER INSTALLATION	11	
MANAGER CONFIGURATION	11	
NETWORK CONFIGURATION	14	
DEPLOYMENT SCENARIO 2 CONFIGURATION GUIDE	17	
MANAGER INSTALLATION AND CONFIGURATION	18	
MANAGER SERVER INSTALLATION (INTERNAL NETWORK)		. 18
MANAGER SERVER CONFIGURATION (INTERNAL NETWORK)		. 18
MANAGER SECURE CONNECTER SERVER INSTALLATION (DMZ NETWORK)		21
MANAGER SECURE CONNECTOR SERVER CONFIGURATION (DMZ NETWORK)		22
NETWORK CONFIGURATION		
SECURE AGENT CONFIGURATION	31	
NOS, PEAKOS, REPURPOS		
NOS CONFIGURATION	31	
PeakOS CONFIGURATION	33	
RepurpOS CONFIGURATION	34	
WINDOWS 10 IOT		
WINDOWS 10 IoT CONFIGURATION		
10ZIG MANAGER GROUP AUTO-POPULATION FOR SECURE CONNECTED DEVICES	39	
CREATE A GROUP FILTERED BY SECURE AGENT REGISTRATION CODE		
TROUBLESHOOTING AND SUPPORT	.44	
APPENDICES	5	
APPENDIX A – 10ZIG MANAGER MANAGEMENT PROTOCOLS WITHOUT USING THE SECUL CONNECTOR	RE	

APPENDIX B - SUPPORTED 10ZIG MANAGER SECURE CONNECTOR FEATURES FOR REMO	DTE LINUX
CLIENTS	
APPENDIX C - SUPPORTED 10ZIG MANAGER SECURE CONNECTOR FEATURES FOR WIND	OWS 10 IoT
CLIENTS	47
APPENDIX D – SPLIT DNS IN NETWORK ENVIRONMENTS	
INTERNAL DNS	
EXTERNAL DNS	52

### **LIST OF FIGURES**

Figure 1 Components of the 10ZiG Manager Application Suite	7
Figure 2 Some of the various management protocols used between the manager and client operating systems.	7
Figure 3 Management protocols communication channels with secure connector in use	. 8
Figure 4 Internal 10ZiG Manager Server Accessible Externally	9
Figure 5 Internal 10ZiG Manager Server and DMZ based Secure Connector Accessible Externally	.9
Figure 6 Deployment Scenario 1 Example Network Diagram	10
Figure 7 Deployment Scenario 2 Example Network Diagram	17



### OVERVIEW 10ZiG Manager Server Web Console Web Console

FIGURE 1 COMPONENTS OF THE 10ZIG MANAGER APPLICATION SUITE

The 10ZiG Secure Connector is a component of the 10ZiG Manager application suite, which can be included at installation and used to tunnel the various management protocols between manager and client over a secure HTTPs connection.



FIGURE 2 SOME OF THE VARIOUS MANAGEMENT PROTOCOLS USED BETWEEN THE MANAGER AND CLIENT OPERATING SYSTEMS.

The Secure Connector is required to be installed when looking to deploy remotely located 10ZiG Thin Clients or devices running the RepurpOS operating system, and where you want them to be managed centrally from either a head office location, Data Center, or Secure environment such as Azure or AWS where the 10ZiG Manager is deployed.





FIGURE 3 MANAGEMENT PROTOCOLS COMMUNICATION CHANNELS WITH SECURE CONNECTOR IN USE .

The Secure Connector could also be deployed for enterprise networks where VLANS or multiple WAN locations are used and networked through security appliances that could potentially block the standard management protocol communication channels being used. Dependent on how these network security appliances are configured, tunneling the traffic through a HTTPs communication channel can help overcome these blockages.

This 10ZiG Manager Secure Connector - Installation Guide for Remote Clients will look at two common deployment scenarios. Other deployment configurations are possible but not covered here.





Deployment Scenario 1 – Internal 10ZiG Manager Server Accessible Externally

FIGURE 4 INTERNAL 10ZIG MANAGER SERVER ACCESSIBLE EXTERNALLY



Deployment Scenario 2 - Internal 10ZiG Manager Server and DMZ based Secure Connector Accessible Externally

FIGURE 5 INTERNAL 10ZIG MANAGER SERVER AND DMZ BASED SECURE CONNECTOR ACCESSIBLE EXTERNALLY

### **DEPLOYMENT SCENARIO 1 CONFIGURATION GUIDE**

In this deployment, the 10ZiG Manager is installed on a single internal server. The Edge Router/Firewall connected to the Internet from where the externally deployed 10ZiG Clients will connect from, is configured to port forward TCP/443 HTTPs traffic inbound to the 10ZiG Manager Server. No outbound rules are required.



FIGURE 6 DEPLOYMENT SCENARIO 1 EXAMPLE NETWORK DIAGRAM



### MANAGER INSTALLATION AND CONFIGURATION

NOTE: If you are using 10ZiG Windows 10 IoT devices with the XTC Agent 2.1.0.0 or newer installed. You will also need to be running the 10ZiG Manager 3.0.5.0 or newer to manage these devices remotely.

If the 10ZiG Manager is not installed or a supported version, please download the latest version from the 10ZiG website at

#### https://www.10zig.com/manager

A password is required for installation, please contact 10ZiG support to obtain the password. For 10ZiG Technical Support contact details please refer to the section on TROUBLESHOOTING AND SUPPORT

#### MANAGER INSTALLATION

- 1. Run the 10ZiG Manager application suite installer to begin the 10ZiG Secure Manager Setup.
- 2. When the **Choose Components** screen is displayed, select components **Server**, **Console**, **Secure Connector**, **Web Console** and press **Next** to continue the setup procedure.

🛅 10ZiG Cloud Manager Setup		– 🗆 X					
Choose Components Choose which features of 10ZiG Cloud Manager you want to install.							
Check the components you war install. Click Next to continue.	nt to install and uncheck the compo	onents you don't want to					
Select components to install:	<ul> <li>✓ Server</li> <li>✓ Console</li> <li>✓ Cloud Connector</li> <li>✓ Web Console</li> </ul>	Description Position your mouse over a component to see its description,					
Space required: 470.7 MB							
Nullsoft Install System v3.03 ——	< Back	Next > Cancel					

3. Click through the rest of the 10ZiG Secure Manager Setup following the prompts to finish the installation.

#### MANAGER CONFIGURATION

1. Run the 10ZiG Secure Manager Settings application from Start > 10ZiG Manager > 10ZiG Cloud Manager Settings.



2. Switch to the **Cloud Connector** configuration settings. On the **Network** screen the **Cloud Connector Port** is set to **443** by default.





3. Switch to the **Console** configuration tab. The default configuration settings are shown below. If you want to block the relaying of traffic to the Web Console Server to prevent external access to the web-based management tool then enable the option **Disable External Web Console Relaying** to prevent this.



4. Switch to the **Manager** configuration tab. The default configuration settings are shown below.



Switch to the Advanced configuration tab. The default configuration settings are shown below. For troubleshooting issues, the Logging Level can be increased from the default info to debug and the output viewed using the 10ZiG Syslog Viewer from Start > 10ZiG Manager > 10ZiG Syslog.



6. When you have checked these settings and happy with the configuration press the **OK** button to close the **10ZiG Cloud Manager Settings** application.

#### **NETWORK CONFIGURATION**

10ZiG Technology recommends that you have minimum prior knowledge on the following:

- Domain Name System (DNS)
- Network Address Translation (NAT)

#### 10ZiG Manager Cloud Connector Site Recommendations

- A static Public IP address required on the WAN interface.
- Use split DNS with an internal DNS SRV record for 10ZiG Manager Server Hostname resolvable to the 10ZiG Manager Server IP address. And use an external DNS A record for 10ZiG Manager Server Hostname resolvable to the static Public IP Address on the WAN interface.
- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- TCP port 443 by default or custom port number configured in 10ZiG Cloud Manager Settings, opened on Firewall from the public internet and forwarded to the 10ZiG Manager Server IP Address.
- You will need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

#### **External Thin Client Site Recommendations**

• A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.

• You may need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

#### WAN Router/Firewall

To allow external access to the 10ZiG Manager through the Cloud Connector, NAT Port Forwarding/Firewall rules should be configured on the Edge Router/Firewall.

Default ports that should be opened are described below. Custom port numbers used, will need to be adjusted and opened accordingly within the WAN router/firewall device.

NOTE: Router/Firewall configuration will vary depending on the manufacturer/model of device being used. Refer to the manufacturer's product documentation for further guidance on implementing this.

Interface	Protocol	Source Address	Source Ports	Destination Address	Destination Ports	NAT IP	NAT Ports
WAN	ТСР	*	*	WAN IP Address	443	IP Address of the 10ZiG Manager Server	443

Firewall / NAT / Port Forward 0												
The NAT configuration has been changed. The changes must be applied for them to take effect.												
Port Forward 1:1 Outbound NPt												
Ru	les											
			Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NAT IP	NAT Ports	Description	Actions
		24	WAN	TCP/UDP			WAN address	21 (FTP)		21 (FTP)		100
		*	WAN	тср			WAN address	4443		443 (HTTPS)		100
		24	WAN	тср			WAN address	3389 (MS RDP)		3389 (MS RDP)		100
		74	WAN	TCP			WAN address	443 (HTTPS)		443 (HTTPS)		100
		*	WAN	TCP/UDP			WAN address					100
		34	WAN	TCP/UDP			WAN address	80 (HTTP)	10.4.20.254	80 (HTTP)		100
		24	WAN	TCP/UDP			WAN address	8080		80 (HTTP)		100
									bbA t	🕽 Add 💼 Delete	🖹 Save	Separator

Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port	Action
WAN	IPv4	ТСР	*	IP Address of the 10ZiG Manager Server	443	PASS

Fi	Firewall / Rules / WAN										
Th Th	The firewall rule configuration has been changed. The changes must be applied for them to take effect.										
Ē	Floating pkg_tinc WAN LAN DMZ IPsec										
R	les	(Drag to Ch	ange Order)								
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions
1				Reserved Not assigned by IANA						Block bogon networks	•
•	*		IPv4 TCP/UDP			10.4.20.254	80 (HTTP)		none	NAT	1.000
			IPv4 TCP				443 (HTTPS)		none	NAT	1.000
-	*		IPv4 TCP				3389 (MS RDP)		none	NAT	<b>₹</b> \000
			IPv4 TCP/UDP				80 (HTTP)		none	NAT	±.≁©⊘∎
•	*		IPv4 TCP/UDP						none	NAT	<b>↓</b> /□0#
			IPv4 TCP				443 (HTTPS)		none	NAT	1.000
-	*		IPv4 TCP/UDP				21 (FTP)		none	NAT	±≠©0∎
									1 Add 1	Add 💼 Delete 🔛 Sa	ve 🕂 Separator

### **DEPLOYMENT SCENARIO 2 CONFIGURATION GUIDE**

In this deployment, the 10ZiG Manager is installed on multiple servers. Internally the Manager Server, Console, and Web Console Server are installed. The Edge Router/Firewall connected to the Internet from where the externally deployed 10ZiG Clients will connect from, is configured to port forward TCP/443 HTTPs traffic inbound to the 10ZiG Manager Cloud Connector Server situated in a DMZ. The DMZ is configured to forward the required traffic Internally to the destination 10ZiG Manager Server. Outbound rules from the internal network are required to forward traffic back to the Cloud Connector in the DMZ.



FIGURE 7 DEPLOYMENT SCENARIO 2 EXAMPLE NETWORK DIAGRAM



### MANAGER INSTALLATION AND CONFIGURATION

NOTE: If you are using 10ZiG Windows 10 IoT devices with the XTC Agent 2.1.0.0 or newer installed. You will also need to be running the 10ZiG Manager 3.0.5.0 or newer to manage these devices remotely.

If the 10ZiG Manager is not installed or a supported version, please download the latest version from the 10ZiG website at

#### https://www.10zig.com/manager

A password is required for installation, please contact 10ZiG support to obtain the password. For 10ZiG Technical Support contact details please refer to the section on TROUBLESHOOTING AND SUPPORT

#### MANAGER SERVER INSTALLATION (INTERNAL NETWORK)

- 1. Run the 10ZiG Manager application suite installer to begin the 10ZiG Cloud Manager Setup.
- 2. When the **Choose Components** screen is displayed, select components **Server**, **Console**, **Web Console** and press **Next** to continue the setup procedure.

10ZiG Cloud Manager Setup		– 🗆 X
Choose Components Choose which features of 10ZiG install.	Cloud Manager you want to	10ZiG.
Check the components you war install. Click Next to continue.	t to install and uncheck the comp	onents you don't want to
Select components to install:	Server Console Cloud Connector Web Console	Description Position your mouse over a component to see its description,
Space required: 470.7 MB		
Nullsoft Install System v3.03	< <u>B</u> ack	Next > Cancel

3. Click through the rest of the 10ZiG Cloud Manager Setup following the prompts to finish the installation.

#### MANAGER SERVER CONFIGURATION (INTERNAL NETWORK)

1. Run the **10ZiG Cloud Manager Settings** application from **Start > 10ZiG Manager > 10ZiG Cloud Manager Settings**.



🔯 Cloud Manager Setting	js			-		×	
File Help							
102iG		Console	Cloud	Web			
Network						^	
Discovery	Select the app communication	propriate adapter to on.					
Advanced	Adapter :	ntel(R) 82574L Gigab	oit Network Connecti	ion (IP: 10.4.20.21)	<b>v</b>		
Image Store	Note: I e	f the computer has W mabled, make certair MgrService.exe' to th	Vindows Firewall 1 to add e exclusion.				
	The remoting Console. TCP	port is used for com port 11132 is the def	imunication with the fualt value.				
		t: 11132 🗘 r					
	Note: C v c	Only change this valu vith another service. I onfigure your consol vort.	e if the port conflicts Make certain to les to use the same				
						_	
	The unique co the Cloud Co	ode for the Manager nnector					
		279ddecb-2670-44	45e-914d-66766b00	8944			
						_	
	Specify to by						
	Security						
	Specify to use older TLS protocols for legacy unit compatibly.						
	Note	By default, the M 1.2 security prot	lanager Server utiliz ocol,				
	WARNING	: Enabling deprec Layers (TLS) mig	ated Transport Secu ht put your Thin Clie	rity ent Ven		. <b>4.7</b> v	
			ОК	Apply	Ca	ncel	

2. Switch to the **Cloud Connector** configuration settings. On the **Network** screen the **Cloud Connector Port** is set to **443** by default.





3. Switch to the **Console** configuration tab. The default configuration settings are shown below.



 Switch to the Manager configuration tab. The default configuration settings are shown below. Make a note or copy the Relay Code displayed here. This is required to be entered in the 10ZiG Manager Cloud Connector Server settings.



Switch to the Advanced configuration tab. The default configuration settings are shown below. For troubleshooting issues, the Logging Level can be increased from the default info to debug and the output viewed using the 10ZiG Syslog Viewer from Start > 10ZiG Manager > 10ZiG Syslog.





6. When you have checked these settings and happy with the configuration press the **OK** button to close the **10ZiG Cloud Manager Settings** application.

#### MANAGER SECURE CONNECTER SERVER INSTALLATION (DMZ NETWORK)

- 1. Run the 10ZiG Manager application suite installer to begin the 10ZiG Cloud Manager Setup.
- 2. When the **Choose Components** screen is displayed, select the **Cloud Connector** component, and press **Next** to continue the setup procedure.

🎦 10ZiG Cloud Manager Setup		_ 🗆 🗙							
Choose Components Choose which features of 10ZiG Cloud Manager you want to install.									
Check the components you war install. Click Next to continue.	nt to install and uncheck the compo	onents you don't want to							
Select components to install:	<ul> <li>Server</li> <li>Console</li> <li>✓ Cloud Connector</li> <li>Web Console</li> </ul>	Description Position your mouse over a component to see its description,							
Space required: 470.7 MB									
Nullsoft Install System v3.03 ——	< Back	Next > Cancel							

3. Click through the rest of the 10ZiG Cloud Manager Setup following the prompts to finish the installation.

#### MANAGER SECURE CONNECTOR SERVER CONFIGURATION (DMZ NETWORK)

- 1. Run the **10ZiG Cloud Manager Settings** application from **Start > 10ZiG Manager > 10ZiG Cloud Manager Settings**.
- 2. Switch to the **Cloud Connector** configuration settings. On the **Network** screen the **Cloud Connector Port** is set to **443** by default.



3. Switch to the Console configuration tab. If Web Console access is required externally, then configure the Web Console Host value with the 10ZiG Manager (Web Console Server) IP Address. If you wish to prevent traffic before relayed between the Cloud Connector and Web Console Server, then you can restrict this usage Enabling the option Disable External Web Console Relaying.



4. Switch to the **Manager** configuration tab. The default configuration settings are shown below. Paste or enter the **Relay Code** from the **10ZiG Manager Server** configured previously here





- Switch to the Advanced configuration tab. For troubleshooting issues, the Logging Level can be increased from the default info to debug and the output viewed using the 10ZiG Syslog Viewer from Start > 10ZiG Manager > 10ZiG Syslog.
- 6. Enable the option Enable On Demand Port Allocation.
- 7. **Starting Port** can be configured with any port number within the range 1025 65535. The default value is starting from port **30000**. If this conflicts with any other applications on the network, it can be changed to a different value.
- 8. Number to Ports by default is set to 250. The number entered here is determined by the number of remote clients that will be connecting simultaneously.in addition to the number of simultaneous VNC/RDP connections. For example, you have 50 remotely deployed 10ZiG Thin Clients and 4 Desktop Support staff that may be shadowing users via VNC/RDP providing support. Enter a value of 54 should provide the required number of ports (30000 30053) to facilitate clients and support sessions. If you stick with the default number of ports 250, then the port range will be (30000 30249).
- 9. **Inactivity timeout** by default is configured to **5** seconds.



🙆 Cloud Manager Setting	IS	-		×
File Help				
102iG.	Server Console Cloud Web			
Network				
Console	Specify the level which to log the Cloud Connector information			
Manager	Logging Level : Debug			
Advanced	Specify to enable on demand port allocation between the Clou and the Manager Server.		ector	
	Enable On Demand Port Allocation			
	Starting Port : 30000 🗘 number			
	Number to Ports : 250 🗘 number			
	Inactivity Timout : 5 🛟 seconds			
	Note: Thin clients will require 1 port for connectivity between the Cloud Connector and the Manager Server. Remote sessions (VNC/ROP) will utilize an additional port for each concurrent session. Please ensure that the appropriate amount of ports are allocated for your system before use.			
	OK Ap	oply	Car	ncel

1. When you have checked these settings and happy with the configuration press the **OK** button to close the **10ZiG Cloud Manager Settings** application.

#### **NETWORK CONFIGURATION**

10ZiG Technology recommends that you have minimum prior knowledge on the following:

- Domain Name System (DNS)
- Network Address Translation (NAT)

#### 10ZiG Manager Cloud Connector Site Recommendations

- A static Public IP address required on the WAN interface.
- Use split DNS with an internal DNS SRV record for 10ZiG Manager Server Hostname resolvable to the 10ZiG Manager Server IP address. And use an external DNS A record for 10ZiG Manager Server Hostname resolvable to the static Public IP Address on the WAN interface.
- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- TCP port 443 by default or custom port number configured in 10ZiG Cloud Manager Settings, opened on Firewall from the public internet and forwarded to the 10ZiG Manager Cloud Connector Server IP Address.
- You will need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.



#### **External Thin Client Site Recommendations**

- A NAT router is required in a typical deployment. Most business grade SOHO routers and above include this function.
- You may need administrative access to the WAN router/firewall device. 10ZiG Technology will not provide support in configuration of this device.

#### WAN Router/Firewall

To allow external access to the 10ZiG Manager through the Cloud Connector, NAT Port Forwarding/Firewall rules should be configured on the Edge Router/Firewall.

Default ports that should be opened are described below. Custom port numbers used, will need to be adjusted and opened accordingly within the WAN router/firewall device.

NOTE: Router/Firewall configuration will vary depending on the manufacturer/model of device being used. Refer to the manufacturer's product documentation for further guidance on implementing this.

**EXTERNAL > INTERNAL** 

Interface	Protocol	Source Address	Source Ports	Destination Address	Destination Ports	NAT IP	NAT Ports
WAN	ТСР	*	*	WAN IP Address	443	IP Address of the 10ZiG Manager Cloud Connector Server (DMZ)	443

Fire	Firewall / NAT / Port Forward 0										
The N The c	The NAT configuration has been changed. The changes must be applied for them to take effect.										
Port	Port Forward 1:1 Outbound NPt										
Rule	s										
		Interface	Protocol	Source Address	Source Ports	Dest. Address	Dest. Ports	NATIP	NAT Ports	Description	Actions
•	<b>x</b> ¢	WAN	TCP/UDP			WAN address	21 (FTP)		21 (FTP)		10
- *	2¢	WAN	тср			WAN address	4443		443 (HTTPS)		
- *	2¢	WAN	TCP			WAN address	3389 (MS RDP)		3389 (MS RDP)		
-	24	WAN	тср			WAN address	443 (HTTPS)		443 (HTTPS)		
	24	WAN	TCP/UDP			WAN address					
•	24	WAN	TCP/UDP			WAN address	80 (HTTP)	10.4.20.254	80 (HTTP)		
- *	24	WAN	TCP/UDP			WAN address	8080		80 (HTTP)		
								and a second		PO Saus	Consentor

Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port	Action
WAN	IPv4	ТСР	*	IP Address of the 10ZiG Manager Cloud Connector Server	443	PASS

Firewall / Rules /	Firewall / Rules / WAN									
The firewall rule configuration The changes must be applied	The firewall rule configuration has been changed. The changes must be applied for them to take effect.									
Floating pkg_tinc	WAN LAN DMZ									
Rules (Drag to Change	Order)									
States Proto	col Source	Port Destination	Port	Gateway Q	ueue Schedule	Description	Actions			
🗰 0/1.32 MIB 🔹	Reserved Not assigned by IANA			• •		Block bogon networks	0			
■ ✓ 3/22.14 IPv4 MIB TCP/	* UDP	* 10.4.20.254	80 (HTTP)	* r	none	NAT				
🔳 🖌 0/240 8 IPv4	тср •		443 (HTTPS)	* 1	none	NAT	1000			
62 /1.61 GIB IPv4	TCP *		3389 (MS RDP)	* r	none	NAT	7%00 <b>0</b>			
V 0./4 K(B IPv4     TCP/	* UDP		80 (HTTP)	* r	none	NAT	1.000 t			
■ ✓ 0./5 KiB IPv4 TCP/	* UDP			* 1	none	NAT	\$100 <b>0</b>			
🔲 👻 0/238.608 IPv4	TCP *		443 (HTTPS)	* r	none	NAT	1/000			
Image: 0 /808 Ki8         IPv4           TCP/         TCP/	* UDP		21 (FTP)	* r	none	NAT	±≠⊡⊘∎			
					t Add t	ldd 💼 Delete 🖺 Sa	ve 🕂 Separator			

DMZ > INTERNAL

Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port	Action
DMZ	IPv4	ТСР	IP Address of the 10ZiG Manager Cloud Connector Server	IP Address of the 10ZiG Manager Server	52500	PASS
DMZ	IPv4	ТСР	IP Address of the 10ZiG Manager Cloud Connector Server	IP Address of the 10ZiG Manager Server	50000	PASS
DMZ	IPv4	ТСР	IP Address of the 10ZiG Manager Cloud Connector Server	IP Address of the 10ZiG Manager Server	8001	PASS

Fi	Firewall / Rules / DMZ 😤 💷 🖻 🕑										
Th Th	The firewall rule configuration has been changed. The changes must be applied for them to take effect.										
FÌ	Floating pkg_tinc WAN LAN DMZ IPsec										
Ru	ıles	(Drag to	Change (	Order)							
		States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedul	Description	Actions
			IPv4 *	DMZ net						Default allow LAN to any rule	
			IPv4 *	DMZ net		WAN net			none	Default allow DMZ to WAN rule	
	~		IPv4 TCP				52500		none	10ZiG Manager	₺₡©₡₶
			IPv4 TCP				8001		none	10ZiG Manager Firmware Updates	
	*		IPv4 TCP				50000		none	10ZiG Manager Web Connector	±∕©⊘∎
										🕈 Add 🧎 Add 🗎 Delete 🔛 :	Save 🕂 Separator

#### INTERNAL > DMZ

Interface	Address Family	Protocol	Source Address	Destination Address	Destination Port Range	Action
LAN	IPv4	ТСР	* IP Address of the 10ZiG Manager Server	IP Address of the 10ZiG Manager Cloud Connector Server	30000 - 30249	PASS

Fire	Firewall / Rules / LAN 🛱 🔟 🗐 📀									
The fir The cł	The firewall rule configuration has been changed. The changes must be applied for them to take effect.									
Floati			IAN LAI	N						
Rules	s (Drag	to Change C	order)							
	States	Protocol	Source	Port	Destination	Port	Gateway	Queue Schedule	Description	Actions
~					LAN Address	80			Anti-Lockout Rule	٠
- ~		IPv4 *	LAN net		WAN net			none	Default allow LAN to WAN rule	≟∥⊡⊘ ∎
- ~		IPv6 *	LAN net						Default allow LAN IPv6 to any rule	÷∕⊂⊻ ∎
• ~		IPv4 *	LAN net						Default allow LAN IPv4 to any rule	≟∕⊡⊻ ∎
- ~		IPv4 TCP/UDP				30000 - 30249		none	10ZiG Manager Cloud Connector	±∕©0 ∎
								A 1	idd 🧎 Add 📋 Delete 🖺 Sav	ve 🕂 Separator

### SECURE AGENT CONFIGURATION

All 10ZiG Thin Client Operating Systems - NOS, PeakOS, RepurpOS - and Windows 10 IoT clients come pre-installed with a Cloud Manager Agent. This section guides you through configuring the Cloud Manager Agent for remotely deployed 10ZiG Thin Clients.

NOTE: 10ZiG Technology offer a service to use a custom configured template provided by the customer, which can be put on ordered Thin Clients during the production phase before shipping. So already pre-configured on arrival to the customer premises. If you are interested in taking advantage of this service, please discuss further with your sales representative.

### NOS, PeakOS, RepurpOS

#### NOS CONFIGURATION



1. From the NOS Control Panel, select Cloud Manager.



 Enter the Hostname (FQDN) or Public IP Address of the 10ZiG Manager Cloud Connector.Server. This is used as an alternative to the secure agent discovering the secure connector using the 'Server Address from a DNS SRV record'. To leverage this connectivity, refer to Appendix D – Split DNS in Network Environments.

😭 Cloud Manager Configuration	👷 Cloud Manager Configuration			
Version: 1.0.06	Version: 1.0.06			
✓ Server Address from DNS SRV record	Server Address from DNS SRV record			
Server Address: tzmgr.company.com Port: 443	Server Address: 81.5.13.124 Port: 443			
Server Certificate error action: accept	Server Certificate error action: accept			
Proxy Server	Proxy Server			
Proxy Address: Port: 0	Proxy Address: Port: 0			
User: Password:	User: Password:			
Keepalive interval (sec.): 55 Test connection	Keepalive interval (sec.): 55 Test connection			
Reconnection timeout (sec.): 30	Reconnection timeout (sec.): 30			
Service status: CONNECTED	Service status: CONNECTED			
To be managed by 10ZiG Cloud Management, the Thin Client need to be registered through a registration code or user credentials.	To be managed by 10ZiG Cloud Management, the Thin Client need to be registered through a registration code or user credentials. Registration			
Debug	Debug			

- 3. If the 10ZiG Manager Server and Cloud Connector are configured and deployed, you can click the **Test Connection** button to check the connection is successful.
- 4. OPTIONAL: You can click the **Registration...** button and add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance. Click the **OK** button when you have completed this.

0	Dialog	X
6	)   Registratio	on code
	Code:	RemoteUsers
	<ul> <li>Credential</li> <li>User name:</li> <li>Password:</li> </ul>	S
		Сапсеl 🖉 Сапсеl

5. When you are happy with the settings on the Cloud Manager Configuration screen you can press the **OK** button to complete this part of the deployment configuration.

(<u>m</u>)

#### **PeakOS CONFIGURATION**

1. From the PeakOS Terminal Properties screen, select Cloud Manager.



1. Enter the Hostname (FQDN) or Public IP Address of the 10ZiG Manager Cloud Connector.Server. This is used as an alternative to the secure agent discovering the secure connector using the 'Server Address from a DNS SRV record'. To leverage this connectivity, refer to Appendix D – Split DNS in Network Environments.

O, TzWsAgent.real	$\mathbf{X}$	O, TzWsAgent.real 🛪
Enable 10ZiG Cloud Management Agent	Version: 1.0.04	Version: 1.0.04
Server Address from DNS SRV record		Server Address from DNS SRV record
Server Address: tzmgr.company.com	Port: 443	Server Address: 81.5.13.124 Port: 443
Server Certificate error action: accept	•	Server Certificate error action:
Proxy Server		Proxy Server
Proxy Address:	Port: 0	Proxy Address: Port: 0
User: Password: *	****	User: Password:
Keepalive interval (sec.): 55	Test connection	Keepalive interval (sec.): 55 Test connection
Reconnection timeout (sec.): 30		Reconnection timeout (sec.): 30
Service status: CONNECTE		Service status: CONNECTED
To be managed by 10ZIG Cloud Management, the Thin registered through a registration code or user credentia Registration	Client need to be als.	To be managed by 10ZIG Cloud Management, the Thin Client need to be registered through a registration code or user credentials.           Registration
Debug     OK     Car	ncel Apply	Debug OK Cancel Apply

2. If the 10ZiG Manager Server and Cloud Connector are configured and deployed, you can click the Test Connection button to check the connection is successful.

3. OPTIONAL: You can click the **Registration...** button and add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance. Click the **OK** button when you have completed this.

0,		Dialog 🛛 🕅
	<ul> <li>Registration</li> </ul>	i code
	Code:	remoteuser
0	Credentials	
1	User name:	
1	Password:	****
		OK Cancel

4. When you are happy with the settings on the Cloud Manager Configuration screen you can press the **OK** button to complete this part of the deployment configuration.





1. Enter the **Hostname (FQDN)** or **Public IP Address** of the **10ZiG Manager Secure Connector Server**. This is used as an alternative to the secure agent discovering the secure connector using the 'Server Address from a DNS SRV record'. To leverage this connectivity, refer to Appendix D – Split DNS in Network Environments.

TzWsAgent.real	🔽 TzWsAgent.real
Version: 1.0.06	Version: 1.0.06
Server Address from DNS SRV record	Server Address from DNS SRV record
Server Address: tzmgr.company.com Port: 443	Server Address: 81.5.13.124 Port: 443
Server Certificate error action: accept	Server Certificate error action: accept
Proxy Server	Proxy Server
Proxy Address: Port: 0	Proxy Address: Port: 0
User: Password:	User: Password:
Keepalive interval (sec.): 55 Test connection	Keepalive interval (sec.): 55 Test connection
Reconnection timeout (sec.): 30	Reconnection timeout (sec.): 30
Service status: DISCONNECTED	Service status: DISCONNECTED
To be managed by 10ZIG Cloud Management, the Thin Client need to be registered through a registration code or user credentials.           Registration	To be managed by 10ZiG Cloud Management, the Thin Client need to be registered through a registration code or user credentials.
Debug	Debug

- 2. If the 10ZiG Manager Server and Secure Connector are configured and deployed, you can click the **Test Connection** button to check the connection is successful.
- 3. OPTIONAL: You can click the **Registration...** button and add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance. Click the **OK** button when you have completed this.

10 Dialog	
Registration	code
Code:	remoteuser
O Credentials User name:	
Password:	*****
	OK X Cancel

4. When you are happy with the settings on the Registration Code Configuration screen you can press the **OK** button to complete this part of the deployment configuration.



### WINDOWS 10 IoT

NOTE: 10ZiG Windows 10 IoT devices must be running 10ZiG XTC Agent 2.1.0.0 or newer to be able to connect remotely using the 10ZiG Manager Secure Connector.

You can check this on your device by right clicking the XTC Agent Tray icon from the Windows system tray.



From the menu displayed, select **About XTC Agent Tray**.





If you do not see this icon in the system tray, then either the XTC Agent is not installed or not currently running. If it is not running but installed, go to **Start > All Programs > 10ZiG XTC Agent > XTC Agent Tray** to start the service. If the XTC Agent tray is not installed or a supported version, please download the latest version from the 10ZiG website at <u>https://www.10zig.com/manager</u>

alternatively contact 10ZiG support to obtain the latest version. For 10ZiG Technical Support contact details please refer to the section on TROUBLESHOOTING AND SUPPORT

#### WINDOWS 10 IOT CONFIGURATION

- 1. Right click the **XTC Agent Tray** icon **E** from the Windows System Tray.
- 2. From the menu displayed select Secure Agent Settings...

	About XTC Agent Tray		
	Cloud Agent Settings		
	Start Service Stop Service	63	
	Advanced		>
	Exit		
	<b></b>		
V	🚖 🕒		
6	<b>0</b>		
	へ EP (小) 10:46 17/09/2020	$\Box$	

3. Enter the **Hostname** or **Public IP Address** of the router with access to the 10ZiG Manager Secure Connector Server.

10ZiG XTC C	loud Ager	nt Settings				×
Cloud Man	agement A	gent settin	igs			
$\sim$	🔽 Enabl	e 10ZiG Clo	oud Manage	ment Agent	:	
S107	Serve	r Address	from DNS SI	RV record		
Server A	ddress:	tzmgr.con	npany.com		Port:	443
Server C	ertificate:	accept		•	Test (	Connection
Status:				CONNECTE	D	
		Proxy set	ttings			
Registra	tion Code:					
			OK	C	ancel	Apply



4. OPTIONAL: You can add a **Registration Code** that can be used by the 10ZiG Manager to auto-populate the device into a group configured with a registration code filter for better organization and easier maintenance.

0ZiG XTC Cloud Agent Settings ×
Cloud Management Agent settings
Server Address from DNS SRV record
Server Address: 81.5.13.124 Port: 443
Server Certificate: accept   Test Connection
Status: CONNECTED
Proxy settings
Registration Code: remoteusers
OK Cancel Apply

5. When you are happy with the settings on the 10ZiG XTC Secure Agent settings screen you can press the **OK** button to complete this part of the deployment configuration.

# **10ZIG MANAGER GROUP AUTO-POPULATION FOR** SECURE **CONNECTED DEVICES**

The 10ZiG Manager can automatically populate registered 10ZiG Thin Client devices into groups for easier visibility and administration for implementing firmware and configuration templates.

10ZiG Manager Console											
File Tools Help				Reading Section Present Section Presen				perfersion of the second			
🎂 😂 🕸 🚀 😰 🚯 🗶	-   😺	16 16 😤 🖉	88 8 4	18 🛛 🖉 🖉	🍰 😼 🦉	1	9 5	• 🎤	🐊 🖬 🔳		
Search (0)	U	Name	▲ IP	MAC	Platform	Model	Version	Template	Templa System Drive	RAM	Last Responded
😑 🚅 Thin Clients (16)	Online	- Cloud Client									
Remote Users Group (0)	<u></u>	DESKTOP-B8GMMC	0 192.168.1.21	00E0C530A616	WIN 10 (x64)	5810QD	2.1.0.5		28.29 GB	3.84 GB	18/09/2020 09:38:55
	Online										
	🖏 👢	10ZiG-5371e8f	192.168.247.128	00E0C5371E8F	NOS	9948qc	CWA2006_16.1.20.2.rc1		20.00 GB	3.84 GB	17/09/2020 22:09:34
	Offline	- Cloud Client									
	4	10ZIG_30a616		00E0C530A616	PKOS	5872qd	12.0.129		1.87 GB	3.78 GB	17/09/2020 16:13:37
	Offline	(13 devices)									
	-	10ZIG_e7de46		EC21E5E7DE46	PKOS	RPOS-02	12.1.134.35		119.24 GB	3.79 GB	15/09/2020 17:24:49
	*6	10ZiG-2ab767		00E0C52AB767	Linux	6072q	16.2.21.rc2		7.28 GB	7.48 GB	16/09/2020 20:30:52
	*	10ZiG-2ab91b		00E0C52AB91B	Linux	6072q	16.2.21.rc2		7.28 GB	3.54 GB	17/09/2020 09:05:00
	*	10ZiG-523ca1b		00E0C523CA1B	NOS	NOS-QV	10.12.167		20.00 GB	7.92 GB	08/09/2020 16:02:25

Internal devices are normally easy to filter, as the two most widely used filters implemented are **Filter by Platform** for the device operating system, and **Filter by IP Address**, which can be useful in VLAN and WAN environments where multiple IP subnets are used.

Thin Client Group - Remote Users Grou	×
Name : Remote Users Group Description :	
Auto-population Filters Client Configuration	
<ul> <li>Filter by Platform</li> <li>Automatically populate this group with thin clients that match the specified platform.</li> <li>Innux (NOS, PKOS, RPOS)</li> </ul>	Filter by IP Address Automatically populate this group with thin clients that have an IP address fitting specified criteria.
<ul> <li>Windows</li> <li>Windows CE</li> </ul>	Edit IP Filter list
Filter by Model Automatically populate this group with thin clients that match the specified model(s). Edit model list	Automatically populate this group with thin clients that have a MAC address fitting specified criteria.
Filter by Version Automatically populate this group with thin clients that match the specified version(s).	Automatically populate this group with thin clients that have computer names fitting specified criteria.
Edit version list	Filter by Cloud Agent Registration Code Automatically populate this group with thin clients that have the specified registration code(s). Edit Registration Codes
	OK Cancel

For deployments of remotely located 10ZiG Thin Clients however this is more problematic as they will be seen in the 10ZiG Manager as coming from various public IP addresses assigned to the WAN interface of their Edge Router/Firewall.

The easiest way to auto populate remote devices into groups is to use the **Registration Code** configured in the client Secure Agent. This can be configured before shipping clients to the users or if already done so, once connected to the 10ZiG Manager by sending a configuration file/template to the client with the **Registration Code** configured.

O Dialog X	10ZiG XTC Cloud Agent Settings X
Registration code   Code: RemoteUsers   O Credentials   User name:   Password:	Cloud Management Agent settings
	Windows 10 IoT

### **CREATE A GROUP FILTERED BY SECURE AGENT REGISTRATION CODE**

- 1. Open the **10ZiG Manager Console**.
- 2. Right click the parent **Thin Clients** group or if you already have some child groups you want the new group to become a sub-group member of, right click on that group and select **New > Group**.



3. At the **Thin Client Group** screen, enter a **Name** for your group and optional **Description**. Under **Auto-population Filters** configure the following:



- a. Enable Filter by Platform and select the Operating System family of the remote devices being grouped.
- b. Enable Filter by Secure Agent Registration Code and click Edit Registration Codes....

Thin Client Group - Remote Users Grou	×
Name : Remote Users Group	
Description :	
Auto-population Filters Client Configuration	
Filter by Platform	Filter by IP Address
Automatically populate this group with thin clients that match the specified platform.	Automatically populate this group with thin clients that have an IP address fitting specified ortheria.
O Windows CE	Filter by MAC Address
Filter by Model Automatically populate this group with thin clients that match the specified model(s).	that have a MAC address fitting specified criteria. Edit MAC list
Edit model list	Filter by Computer Names
Filter by Version Automatically populate this group with thin clients that match the specified version(s).	Automatically populate this group with thin clients that have computer names fitting specified criteria.
Edit version list	Filter by Cloud Agent Registration Code     Automatically populate this group with thin clients that     have the specified registration code(s).     Edit Registration Codes
	OK Cancel

4. Once the **Edit Registration Codes...** button is pressed the **Filter Registration Codes** screen is displayed. Click the **Add** button to create a new pattern and enter the value configured in the 10ZiG Thin Clients Secure Manager Agent **Registration Code** field here.

Pattern			Include
REMOTEU	SERS		
Add	Edit	Remove	
Add (ou can use single chara characters.	Edit the wildcard acter and '*' f	Remove d characters '? to match any r	' to match any number of



- 5. Once you are happy the **Registration Code** patterns are configured correctly. Press the **OK** button to close the Filter Registration Codes screen.
- 6. Press the **OK** button on the Thin Client Group screen and the new group should appear and be configured ready for devices to auto-populate.

10ZiG Manager Console												
File Tools Help			8 6 9 4	*	1.01	🕸 🕸   🖻	Ø \$		<u>ू</u> ब		ца 1. с. 7 Г. с	7
Search (0)	U	. Name	▲ IP	MAC	Platform	Model	Version	Template	Templa	System Drive	RAM	Last Responded
Remote Users Group (1)	i Online	DESKTOP-B8GMMC	0 192.168.1.21	00E0C530A616	WIN 10 (x64)	5810QD	2.1.0.5			28.29 GB	3.84 GB	18/09/2020 10:37:28

- 7. If the devices do not auto-populate to the group automatically you can check the following:
  - a. Force a Re-Register by selecting the client or client(s) you want to correctly auto-populate and either press

the **Re-Register** button on the toolbar or right click and from the menu displayed select the option Re-Register.

Refresh
Reregister
Properties

- b. Reboot the client to force it to re-register on boot.
- c. Check the **Registration Code** is correct in both the client **Secure Agent** on the devices and group **Filter by Secure Agent Registration Code** and then attempt the above again.

Unfortunately, it is not possible to filter Linux and Windows 10 IoT devices in the same group, as you can only select either Linux or Windows in the **Filter by Platform** option.

What you can do instead is create a group for the purpose of organizing the devices and then subgroups within that group can be used for splitting the different platforms.



You can have a single group for the Linux platform, which would put any NOS, PeakOS, RepurpOS devices into it. But this could cause issues mixing those devices in the same group further down the road if you want to assign automatic templates to the group, as these differ between the different operating systems and firmware.

It is not an issue if you do not use **Automatic Client Configuration**, or **Auto Update Firmware**. But if you do intend to do this then you want to split the NOS, PeakOS, RepurpOS devices into their own specific groups.

Create the group with the **Filter by Platform** and **Filter by Secure Agent Registration Code** items configured as described above but also configure the **Filter by Version**.

Filter by Version Automatically populate this group with thin clients that match the specified version(s).
Edit version list

- 1. Enable Filter by Secure Agent Registration Code and click Edit version list....
- 2. Once the **Edit version list...** button is pressed the **Filter Thin Client Versions** screen is displayed. Click the **Add** button to create a new pattern and enter the prefix value from the below table along with a \* (wildcard) to filter that specific operating system.

Pattern				Include
12*				$\checkmark$
Add	Edit	Remove		
Add	Edit	Remove	?' to mat	ch anv
Add You can use single chara characters.	Edit the wildcard acter and '*' t	Remove d characters ' to match any	?' to mat number	ch any of
Add You can use single chara characters. NOTE: The ' matching th matching cl	Edit e the wildcard acter and '*' t "Include" che ne pattern ar ients are exci	Remove d characters ' to match any ckbox detern e included; if luded.	?' to mat number nines if c	ich any of lients ked

1. Once you are happy the **Thin Client Version** patterns are configured correctly. Press the **OK** button to close the Filter Thin Client Versions screen.

Operating System	Firmware Version Format	Pattern
NOS (32bit)	10.XX.XXX	10*
NOS (64bit)	16.XX.XXX	16*
PeakOS	12.XX.XXX	12*
RepurpOS	12.XX.XXX	12*

NOTE: RepurpOS and Peak OS use the same Firmware Version numbering so if you come across a situation where both these operating systems are in use and you want to filter these out similar to as shown above, then for the RepurpOS devices group you can also use the **Filter by Model** option and configure the pattern to match the platform name prefix **RPOS\***.

<sup>10</sup>ZiG Technology | US P: (866) 865-5250 E: info@10ZiG.com | EMEA P: +44 (0) 116 214 8650 E: info@10ZiG.eu

### **TROUBLESHOOTING AND SUPPORT**

If your having difficulties with deploying a Secure Connector environment or managing remotely deployed 10ZiG Thin Clients, then contact the Technical Support team covering your region for further assistance.

Please have a MAC address of one of your devices available when contacting the Technical Support teams with new support cases.

10ZiG Technology

North America (Rest of the world): P: +1(866)865-5250

E: <u>support@10zig.com</u>

EMEA:

P: +44(0)116 2148661

E: <u>support@10zig.eu</u>

For further information on the 10ZiG Manager Application Suite, you can also look towards our YouTube channel that hosts videos on this subject and our other available products. Usefull videos to look out for are noted below:

Introduction & Tour – PeakOS, NOS, & Windows Endpoint Management Overview

(https://www.youtube.com/watch?v=Le5IXQv6Jlc)

Installation Deployment Best Practices for Remote Management and Configuration of 10ZiG Thin and Zero Clients

(https://www.youtube.com/watch?v=QPKU69BVry4&t=12s)

<u>PeakOS / NOS Endpoint Deployment, Management and Configuration Best Practices</u> (https://www.youtube.com/watch?v=Hap5yHmMj4A)

### **APPENDICES**

### APPENDIX A – 10ZiG MANAGER MANAGEMENT PROTOCOLS WITHOUT USING THE SECURE CONNECTOR

DESCRIPTION	OPERATING SYSTEM(S)	PROTOCOL	PORT(S)
The Manager Console will register one of the ports within this range for notifications.	-	ТСР	1113 - 11147
Discovery port for Thin Clients (Windows & Linux)	WINDOWS	UDP	52500
Used for querying information from and perform operations on Thin Clients (Linux)	LINUX	ТСР	80, 443
Used for publishing firmware updates to Thin Clients (Linux)	LINUX	ТСР	8001
RPC port used for performing remote operations and queries on Thin Clients. (Windows)	WINDOWS	ТСР	52510
RPC port used to enable the Thin Clients to notify the Manager when they come online / offline (Windows)	WINDOWS	ТСР	52511

### **APPENDIX B – SUPPORTED 10ZIG MANAGER** SECURE

### CONNECTOR FEATURES FOR REMOTE LINUX CLIENTS

FEATURE         (YES/NO)           IMAGE MANAGEMENT         NO           BACKUP         NO           RESTORE         NO           SYSTEM OPERATIONS         YES           REBOOT         YES           SHUTDOWN         YES           CONFIGURATION         YES           RETRIEVE         YES           SEND         YES           GENERATE TEMPLATE         YES           SEND         YES           GENERATE TEMPLATE         YES           CLIENT AUTOMATIC NAMING         YES           FIRMWARE UPDATES         YES           VIC REMOTE SHADOWING         YES           SCHEDULED TASKS         YES           POWER ON CLIENT         YES           SHUTDOWN CLIENT         YES           SHUTDOWN CLIENT         YES           SHUTDOWN CLIENT         YES           SHUTDOWN CLIENT         YES           APPLT TEMPLATE CONFIGURATION         YES           RESET TO FACTORY DEFAULTS         YES		SUPPORTED
IMAGE MANAGEMENT         Image management           EACKUP         NO           RESTORE         NO           SYSTEM OPERATIONS         VES           REBOOT         YES           SHUTDOWN         YES           CONFIGURATION         YES           CONFIGURATION         YES           RETRIEVE         YES           GENERATE TEMPLATE         YES           APPLY TEMPLATE         YES           CLIENT AUTOMATIC NAMING         YES           FIRMWARE UPDATES         YES           VIC REMOTE SHADOWING         YES           SHUDDOWN CLIENT         YES           SHUDDOWN OLIENT         YES           SHUDDOWN OLIENT         YES           SHUDDOWN OLIENT         YES           SHUDDOWN OLIENT         YES           SHUDDOWN CLIENT         YES           SHUDDOWN CLIENT         YES           SHUDDOWN CLIENT         YES           SHUDDOWN CLIENT         YES           SHUTDOWN CLIENT         YES	FEATURE	(YES/NO)
IMAGE MANAGEMENT         Current and the second		
BACKUP     NO       RESTORE     NO       SYSTEM OPERATIONS     YES       REBOOT     YES       SHUTDOWN     YES       CONFIGURATION     YES       RETRIEVE     YES       SEND     YES       GENERATE TEMPLATE     YES       REST TO FACTORY DEFAULT SETTINGS     YES       CLIENT AUTOMATIC NAMING     YES       FIRMWARE UPDATES     YES       SKHEDULED TASKS     YES       POWER ON CLIENT     YES       SHUTDOWN CLIENT     YES       SHUTDOWN IGURATION     YES       UPDATE DEVICE FIRMWARE     YES       SHUTDOWN OLIENT     YES       SHUTDOWN IGURATION     YES       SHUTDOWN CLIENT     YES       SHUTDOWN IGURATION     YES       SHUTDOWN ICLIENT     YES	IMAGE MANAGEMENT	
RESTORE     NO       SYSTEM OPERATIONS     YES       REBOOT     YES       SHUTDOWN     YES       CONFIGURATION     YES       RETRIEVE     YES       SEND     YES       GENERATE TEMPLATE     YES       APPLY TEMPLATE     YES       CLIENT AUTOMATIC NAMING     YES       FIRMWARE UPDATES     YES       SYCEBOUT CLIENT     YES       POWER ON CLIENT     NO       REBOOT CLIENT     YES       SHUTDOWN NCLIENT     YES       UPDATE DEVICE FIRMWARE     YES       APPLT TEMPLATE CONFIGURATION     YES       SHEDOLED TAKKE     YES	BACKUP	NO
SYSTEM OPERATIONSYESREBOOTYESSHUTDOWNYESCONFIGURATIONYESRETRIEVEYESSENDYESGENERATE TEMPLATEYESGENERATE TEMPLATEYESCLIENT AUTOMATIC NAMINGYESCLIENT AUTOMATIC NAMINGYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTYESSHUTDOWN CLIENTYESLUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATEYESREBOOT CLIENTYESSHUTDOWN CLIENTYESAPPLT TEMPLATE CONFIGURATIONYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYESAPPLT TEMPLATE CONFIGURATIONYESREBOT TO FACTORY DEFAULTYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	RESTORE	NO
REBOOTYESSHUTDOWNYESCONFIGURATIONYESRETRIEVEYESSENDYESGENERATE TEMPLATEYESAPPLY TEMPLATEYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTYESSHUTDOWN CLIENTYESSHUTDOWN CLIENTYESAPPLT TEMPLATE CONFIGURATIONYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYESSHEDOT CLIENTYESSHUTDOWN CLIENTYESSHUTDOWN CLIENTYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYESRESET TO FACTORY DEFAULTYES	SYSTEM OPERATIONS	
SHUTDOWNYESCONFIGURATIONYESRETRIEVEYESSENDYESGENERATE TEMPLATEYESAPPLY TEMPLATEYESRESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTYESSHUTDOWN CLIENTYESLUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATEYESSHUTDOWN CLIENTYESREBOT CLIENTYESRESET TO FACTORY DEFAULTYESSHUTDOWN CLIENTYESRESET TO FACTORY DEFAULTYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	REBOOT	YES
CONFIGURATIONCRETRIEVEYESSENDYESGENERATE TEMPLATEYESAPPLY TEMPLATEYESRESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYESRESET TO FACTORY DEFAULTYES	SHUTDOWN	YES
RETRIEVEYESSENDYESGENERATE TEMPLATEYESAPPLY TEMPLATEYESRESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYESRESET TO FACTORY DEFAULTYES	CONFIGURATION	
SENDYESGENERATE TEMPLATEYESAPPLY TEMPLATEYESRESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYESRESET TO FACTORY DEFAULTYES	RETRIEVE	YES
GENERATE TEMPLATEYESAPPLY TEMPLATEYESRESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSNOPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	SEND	YES
APPLY TEMPLATEYESRESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	GENERATE TEMPLATE	YES
RESET TO FACTORY DEFAULT SETTINGSYESCLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	APPLY TEMPLATE	YES
CLIENT AUTOMATIC NAMINGYESFIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSYESPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	RESET TO FACTORY DEFAULT SETTINGS	YES
FIRMWARE UPDATESYESVNC REMOTE SHADOWINGYESSCHEDULED TASKSPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	CLIENT AUTOMATIC NAMING	YES
VNC REMOTE SHADOWINGYESSCHEDULED TASKSNOPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	FIRMWARE UPDATES	YES
SCHEDULED TASKSNOPOWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	VNC REMOTE SHADOWING	YES
POWER ON CLIENTNOREBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	SCHEDULED TASKS	
REBOOT CLIENTYESSHUTDOWN CLIENTYESUPDATE DEVICE FIRMWAREYESAPPLT TEMPLATE CONFIGURATIONYESRESET TO FACTORY DEFAULTYES	POWER ON CLIENT	NO
SHUTDOWN CLIENT     YES       UPDATE DEVICE FIRMWARE     YES       APPLT TEMPLATE CONFIGURATION     YES       RESET TO FACTORY DEFAULT     YES	REBOOT CLIENT	YES
UPDATE DEVICE FIRMWARE     YES       APPLT TEMPLATE CONFIGURATION     YES       RESET TO FACTORY DEFAULT     YES	SHUTDOWN CLIENT	YES
APPLT TEMPLATE CONFIGURATION     YES       RESET TO FACTORY DEFAULT     YES	UPDATE DEVICE FIRMWARE	YES
RESET TO FACTORY DEFAULT YES	APPLT TEMPLATE CONFIGURATION	YES
	RESET TO FACTORY DEFAULT	YES

### APPENDIX C – SUPPORTED 10ZiG MANAGER SECURE CONNECTOR FEATURES FOR WINDOWS 10 IOT CLIENTS

	SUPPORTED
FEATURE	(YES/NO)
WRITE PROTECTION	
ENABLE WRITE FILTER	YES
DISABLE WRITE FILTER	YES
IMAGE MANAGEMENT	
CLONE SYSTEM IMAGE	NO
DEPLOY SYSTEM IMAGE	NO
BACKUP	NO
RESTORE	NO
SYSTEM	
LOGOFF CURENT USER	YES
REBOOT	YES
SHUTDOWN	YES
WINDOWS CLIENT ADMINISTRATION	
LOCAL ADMINISTRATOR PASSWORD	YES
AUTOLOGON SETTINGS	YES
MANAGE UPDATES	YES
EXECUTE UPDATES	YES
VNC PROMPT ON CONNECT	YES
CONNECT USING RDP	YES
LOCAL PROCESSES	YES
LOCAL SYSTEM DRIVE	NO
CONFIGURATION	

RETRIEVE	YES
SEND	YES
CLIENT AUTOMATIC NAMING	YES
XTC AGENT UPDATES	YES
VNC REMOTE SHADOWING	YES
SCHEDULED TASKS	
POWER ON CLIENT	NO
LOGOFF ACTIVE USER	YES
REBOOT CLIENT	YES
SHUTDOWN CLIENT	YES
UPDTE XTC AGENT ON CLIENT	YES
DEPLOY SYSTEM IMAGE	NO
EXECUTE UPDATE	YES



### **APPENDIX D – SPLIT DNS IN NETWORK ENVIRONMENTS**

Split DNS is a useful implementation method that allows for a single hostname to be used and resolve to a Private IP Address when on the internal LAN network and to a different Public WAN IP Address when located externally for remote access.

Many client applications such as Microsoft Outlook commonly use a FQDN (Fully Qualified Domain Name) to connect to an application server (i.e. Microsoft Exchange). For 10ZiG Thin Clients this can be used to connect devices to the 10ZiG Manager Server for centralized administration

#### **INTERNAL DNS**

The resolution of the DNS address tzmgr.company.com to the IP address 192.168.1.147 and the subsequent connection between the 10ZiG Thin Client and the 10ZiG Manager Secure Connector will be accomplished as follows.



- 1. Launch the **Microsoft DNS Manager** on your internal DNS Server from the **Administrative Tools** Start menu folder or from the **Server Manager Console**.
- 2. Expand the DNS domain tree to navigate to navigate to the **\_tcp** subdomain in the **Forward Lookup Zones** of your domain as pictured below.

🍰 DNS Manager				- 0	×
File Action View Help					
🗢 🌩 🖄 💼 🗎 🖬 🖓	1				
<ul> <li>DNS</li> <li>DC</li> <li>Forward Lookup Zones</li> <li></li></ul>	Name gc kerberos kpasswd ldap	Type Service Location (SRV) Service Location (SRV) Service Location (SRV) Service Location (SRV)	Data [0][100][3268] dc.10zigde [0][100][88] dc.10zigdemo [0][100][464] dc.10zigdem [0][100][389] dc.10zigdem	Timestamp 17/09/2020 16:00:00 17/09/2020 16:00:00 17/09/2020 16:00:00 17/09/2020 16:00:00	



3. Click the **New Record** toolbar button to begin creating a new record.

Elle       Action       View       Help            ←          ←           ←           ←           ←             Type           Data           Timestamp             ✓            DC           _gc           Service Location (SRV)           [0][100][3268] dc.10zigdem           17/09/2020 16:00:00             ✓           Fonward Lookup Zones           _gc           Service Location (SRV)           [0][100][3268] dc.10zigdem           17/09/2020 16:00:00             ✓           Inzestamp           _gc           Service Location (SRV)           [0][100][3268] dc.10zigdem           17/09/2020 16:00:00             ✓           Inzestamp           _gc           Service Location (SRV)           [0][100][464] dc.10zigdem           17/09/2020 16:00:00             ✓           _ge         _sites           _ge           _ge           17/09/2020 16:00:00             ✓           _ge	DNS Manager				– 🗆 ×	(
A service Location (SRV)      Bervice Location (SR	<u>File Action View H</u> elp					
DNS       New Record       Type       Data       Timestamp         Image: Construction of the system       Forward Lookup Zones       Service Location (SRV)       [0][100][3268] dc.10zigdem       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Service Location (SRV)       [0][100][464] dc.10zigdem       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Service Location (SRV)       [0][100][464] dc.10zigdem       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Service Location (SRV)       [0][100][389] dc.10zigdem       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Service Location (SRV)       [0][100][389] dc.10zigdem       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Image: Construction of the system       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Image: Construction of the system       17/09/2020 16:00:00         Image: Construction of the system       Image: Construction of the system       Image: Construction of the system       17/09/2020 16:00:00         Image: Construction of the system       Image: Consystem       Image: Construction of the system	🗢 🔿 📶 🖾 🍳 🗟 🔳 👔	Ĩ				
	DNS N DC Forward Lookup Zones	ew Record	Type Service Location (SRV) Service Location (SRV) Service Location (SRV) Service Location (SRV)	Data [0][100][3268] dc.10zigde [0][100][88] dc.10zigdemo [0][100][464] dc.10zigdem [0][100][389] dc.10zigdem	Timestamp 17/09/2020 16:00:00 17/09/2020 16:00:00 17/09/2020 16:00:00 17/09/2020 16:00:00	

4. The Resource Record Type dialog window will appear. Scroll down list to find and select **Service Location (SRV)**, then click the **Create Record...** button.

Resource Record Type	×
Select a resource record type:	
Route Through (RT) Service Location (SRV)	^
Signature (SIG)	
Well Known Services (WKS)	
X.25	*
Description:	
Service (SRV) record. Allows administrators to use several servers for a single DNS domain, to easily move a TCP/IP service from one host to another host with administration, and to designate some service provider hosts as primary servers for a service and other hosts as backups. DNS clients that use a SRV-type query ask for a specific TCP/IP service and protocol mapped to a specific DNS domain and receive the names of any available servers. (RFC 2052)	~
Create Record Cancel	

- 5. Specify the record details as pictured below (adjust for your own domain details and host addressing).
  - a. Service: \_tzmgr\_discovery
  - b. Protocol: \_tcp
  - c. Port number: Specify the port used by the Secure Connector (default **443**)

d. Host offering this service: Enter the host name of the server where the Secure Connector has been installed.

Domain:	_tcp.10zigdemo.local	
Service:	_tzmgr_discovery	``
Protocol:	_tcp	`
Priority:	0	
Weight:	0	
Port number:	443	
Host offering this	service:	
tzmgr.10zigdemo	local	
Allow any aut name. This se	henticated user to update all DNS records with the tting applies only to DNS records for a new name.	same

- 6. When you have completed the configuration press **OK** to close and add the new record.
- 7. You can then if you wish to check that the host name of the server where the Secure Connector has been installed has the required (A) record created for it. In this example we have one for **tzmgr** that resolves to 192.168.1.147 internally.

• 🔿 🛛 📷 🖾 📾 🔚 🖬 💼	00			
DNS DC DC Solution DC DC DC DC DC DC DC DC DC DC DC DC DC	Name msdcs sites tcp udp DomainDnsZones ForestDnsZones	Туре	Data	Timestamp
udp	(same as parent folder)	Start of Authority (SOA)	[283], dc.10zigdemo.local	static
> 🔛 DomainDnsZones	(same as parent folder)	Name Server (NS)	dc.10zigdemo.local.	static
> 🧾 ForestDnsZones	(same as parent folder)	Host (A)	10.4.20.25	17/09/2020 16:00:00
> 🧾 Reverse Lookup Zones	Citrix-DDC	Host (A)	10.4.20.28	11/09/2020 14:00:00
> 🧾 Trust Points	Citrix-Server	Host (A)	10.4.20.28	16/10/2019 21:00:00
> 🧮 Conditional Forwarders	dc	Host (A)	10.4.20.25	static
	DESKTOP-CTC8BBD	Host (A)	10.4.20.30	21/10/2019 11:00:00
	DESKTOP-R3LK2HE	Host (A)	10.4.20.30	21/10/2019 14:00:00
	HORIZON	Host (A)	10.4.20.27	11/09/2020 14:00:00
	vcenter	Host (A)	10.4.20.26	static
	W10_HDX01	Host (A)	10.4.20.32	21/10/2019 17:00:00
	WIN-2K16-HZN01	Host (A)	10.4.20.31	21/10/2019 12:00:00
	WIN10_HZN01	Host (A)	10.4.20.30	21/10/2019 11:00:00
	tzmgr	Host (A)	192.168.1.147	



#### **EXTERNAL DNS**

When access is required from a remote location, the connection can no longer be established directly to the 10ZiG Manager Secure Connectors internal IP address. Instead, the DNS address tzmgr.company.com should now resolve to the Public IP address of the WAN router connected to the 10ZiG Manager Secure Connector Server LAN network. This requires that the external Domain Name Server resolves pbx.company.com to the relevant Public IP address.



Since the 10ZiG Thin Client and 10ZiG Manager Secure Connector Server are no longer on the same network the connection is established through the WAN Router/Firewall, which will be configured for port forwarding to allow the 10ZiG Thin Client to register with the 10ZiG Manager Secure Connector Server.

#### CONFIGURE AN EXTERNAL DOMAIN NAME PROVIDER FOR REMOTE CONNECTIVITY

1. Login to your external Domain Name provider.

Domains & S	5L				Adjust Destination
company.c	om				
Details Subdo	omains Privacy & Cor	tact Details Renewal & Tr	ransfer Nameserver	DNS	
Search sub	domains	Q			Create Subdomain
					3 of 10000 used
					> Add subdomain
		Sort t	y Alphabetically (A-Z)	~	
DOMAIN	S	TATUS		ACTIONS	
No subdomains fo	ound. > Add subdomain				

2. Create a Subdomain that will match the Hostname you are using. In this example we are using **tzmgr.company.com**.

Create Subdomain	×
A subdomain is an additional division of your domain. You can use subdomains to make specific content accessible directly. Subdomains are structured according to the pattern subdomain-name.domain-extension.	
Subdomain Name       tzmgr       .company.com	
Create another subdomain Save Cancel	

3. Next you will need to re-direct traffic destined for **tzmgr.company.com** to the Public IP Address of the WAN router connected to the 10ZiG Manager Secure Connector Server network.

Domains & SSL		Adjust Destination
tzmgr.com	ipany.com	
Details 🔅 Ə Back to shlat	.co.uk ≯ DNS	
Tip: With MyWebsite;	you can easily create a website or online shop for your domain t	tzmgr.shlab.co.uk > Create website
Status	Active	
Гуре	Subdomain	
Destination	Domain not in use > Use Your Domain	
Email addresses	> Create	
SSL Certificate	<ul> <li>No SSL certificate assigned</li> <li>Activate SSL encryption</li> </ul>	
Contract	8578774 - Instant Domain Registration	
Reset domain	Reset DNS or usage	
		a menar stilab zo uk



4. Select the option **Forward Domain**.

> Domains & SSL > tzmgr.com	pany.com tion	
Domain not in use		
Create Website	Create your own website easily using our user-friendly editor, customisable layouts and imag all business sectors.	es for >
Connect a Website	Connect your domain to a website created with a IONOS application.	>
Forward Domain	Forward the visitors of your domain to a different website.	>
DNS	Create and edit user-defined DNS records, such as A/AAAA, TXT and CNAME records.	>
Connect to External Page	Connect your domain to your page on an external website or social media service.	>
Create an email address	Set up an email address that matches your domain, e.g. name@tzmgr.shlab.co.uk	>
Reset domain	Reset DNS settings or domain usage settings to IONOS default values. You can then edit then again.	>
Connect to Webspace	This contract does not contain webspace. To add webspace, please switch to another contract.	Change contract

5. Enter the **Public IP Address of the WAN router** connected to the 10ZiG Manager Secure Connector Server network as the **Redirect Destination**. Press **Save** to update sub-domain destination.

Type	O Your domain
	Arbitrary URL
Redirect to destination	81.5.13.124
	The destination of a redirect may be an arbitrary domain or a valid URL
	Please note. To use SSL encryption, it must be enabled for the forwarding destination.
	Also set up for www.subdomain
Redirect type	O HTTP redirect (recommended)
	Automatically redirects your domain to the destination domain The internet address (URL) of your destination domain will appear in your browser's address bar.
	Frame redirect
	Automatically redirects your domain to the destination domain However, the internet address (URL) of your domain will still remain visible in your browser's address bar as the content is disclowed in a frame.



6. The redirection should now be configured. Please note depending on the Domain name provider it may take some time for DNS changes to propagate fully.

Domains & SSL	
tzmgr.comp	any.com
Details > Back to shlab.co.u	ik > DNS
Status	Active
Туре	Subdomain
Destination	Redirect Adjust Destination
Target	http://81.5.13.124 > Adjust Domain Forwarding
Email addresses	> Create
SSL Certificate	No SSL certificate assigned     Activate SSL encryption
Contract	8578774 - Instant Domain Registration
Reset domain	> Reset DNS or usage
Delete Subdomain	× Delete

NOTE: Configuration of external Domain Name services will vary depending on the provider you are using. Please refer to the providers specific documentation on implementing any of the above if differences in configuration are seen when trying to implement this.



THIS PAGE IS INTENTIONALLY BLANK