191100016901000014181480 191100016901

Technical Guide



0001011011

Download Portal

Feature Overview and Configuration Guide

Introduction

This guide describes the Download Portal and how to configure it.

The Download Portal lets administrators offer resources to network users, protected by authentication. The resources could include software installers and setup guidelines, for example a remote access client along with setup instructions, like this:

Download Portal		
Welcome to the Download Portal.		
Software & Configuration Download OpenVPN client configuration file	vpn_client_conf.ovpn	Download
Bookmarks		
Company website	https://alliedtelesis.com	

The Download Portal has two user types, administrators and users.

Download Portal Administrators:

- define the files and links they wish to display on the Download Portal page.
- set up an authentication mechanism that controls access to the Download Portal through usernames and passwords.
- provide users with a URL to subsequently navigate to the Download Portal and retrieve the necessary files and links that they need.

Download Portal Users:

- navigate to the Download Portal (using a link provided by Admin)
- login to the Download Portal page
- download resources from the Download Portal page



Products and software version that apply to this guide

This guide applies to AlliedWare Plus[™] products that support the Download Portal running version **5.5.4-0.1** or later and Device GUI version **2.17** or later. To see whether your product supports this feature, see the following documents:

- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com

Licensing

This feature is part of the standard feature set of AlliedWare Plus and therefore there are no licensing requirements.

Contents

Introduction	.1
Products and software version that apply to this guide	2
Licensing	2
Setting up the Download Portal using the CLI	.4
Adding resources for clients to access on the Download Portal	4
Configuring the listen addresses and ports for client connections (HTTPS)	5
Configuring the RADIUS server	6
Configuring a firewall	8
Configuring an HTTP trustpoint	9
Setting up the Download Portal using the Device GUI1	0
Create separate IP address/port pairs for the Device GUI and the Download Portal1	0
Adding resources for clients to access on the Download Portal1	1
Create users who can access the Download Portal1	4
Checking the Download Portal configuration1	6
Creating firewall rules for exclusive Download Portal user access1	7
How to see the HTTP and HTTPS settings1	9
How do users access the Download Portal?2	20

Setting up the Download Portal using the CLI

This section describes setting up and configuring the Download Portal using the CLI. It includes:

- "Adding resources for clients to access on the Download Portal" on page 4
- Configuring the listen addresses and ports for client connections (HTTPS)" on page 5
- "Configuring the RADIUS server" on page 6
- "Configuring a firewall" on page 8
- "Configuring an HTTP trustpoint" on page 9

Adding resources for clients to access on the Download Portal

1. Add resources to the device

These are the files that you want to make available. For example, to copy a file from a USB stick:

awplus# copy usb:vpn_client_conf.ovpn flash

2. Enter Download Portal mode

```
awplus# configure terminal
awplus(config)# download-portal
awplus(config-download-portal)#
```

3. Configure the resource

These specifies that the files will be displayed in the Download Portal page:

```
awplus(config-download-portal)# file <file-path> [sha256sum <hex-string>]
[description <file-description>]
```

The sha256-sum is used to check the integrity of the file. For example:

```
awplus(config-download-portal)# file flash:/vpn_client_conf.ovpn
sha256sum albed1569bef6b9f8958bf8993ef53bf7c2f62a1833fe41f14
description "OpenVPN client configuration file"
```

4. Configure the URIs (Uniform Resource Identifier)

These are links to external resources that will be displayed in the Download Portal page

awplus(config-download-portal)# uri <uri-link> [description <uri description>]

For example:

```
awplus(config-download-portal)# uri https://alliedtelesis.com description "Allied
Telesis website"
```

Configuring the listen addresses and ports for client connections (HTTPS)

The **secure-listen** command must be configured to set the addresses and ports that the Download Portal HTTP service will listen on for clients connections.

The IP/port configured as the secure-listen address, or FQDN name that points to that IP, is provided to Download Portal Users to navigate to the Download Portal and retrieve the necessary files and links that they need.

1. Consider the HTTP server port options

By default, the device's HTTP server (used by the Device GUI), uses the standard HTTPS port 443, and it is accessible on any of the device's IP addresses. This means it is not available for the Download Portal to use. In order to use the standard HTTPS port (443) for the Download Portal, the HTTP server must be configured to use a different port or restricted to use the standard port on an address that is not used by the Download Portal.

To change the HTTP server to use an alternative to the standard HTTPS port, use the following command:

awplus(config)# http secure-port 10443

To change the HTTP server to use the standard HTTPS port but restricted to a specific IP address assigned to the device, use the following commands:

```
awplus(config)# http secure-port none
awplus(config)# http secure listen 192.168.1.1 443
```

Note: Changes to default HTTP ports should be configured before the Download Portal securelisten configuration is done.

2. Configure the secure-listen address for the Download Portal

The IP specified must already exist on an interface. For example, if you want people to access the Download Portal on 10.0.0.1 and the standard port for HTTPS:

```
awplus(config)# download-portal
awplus(config-download-portal)# secure-listen 10.0.0.1 443
```

3. Enable the Download Portal

awplus(config-download-portal)# enable

Configuring the RADIUS server

Download Portal users are authenticated using the AAA authentication service. The authentication group can use RADIUS or LDAP. For information on LDAP, see the LDAP Feature Overview and Configuration Guide.

The two RADIUS server options are local and external.

Local RADIUS server

1. Enable the local RADIUS server

AlliedWare Plus firewalls and routers include a built-in local RADIUS server, which can provide the authentication service for the Download Portal.

```
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
```

2. Configure users

```
awplus(config-radsrv)# user <username> password <password>
awplus(config-radsrv)# exit
```

3. Configure the host

This uses the local host, which is 127.0.0.1, with the default key, which is 'awplus-local-radius-server':

awplus(config)# radius-server host 127.0.0.1 key awplus-local-radius-server

4. Set the Download Portal to use the RADIUS group for authentication

awplus(config)# aaa authentication download-portal default group radius

For more information about how to configure the local RADIUS server, see the Local RADIUS Server Feature Overview Guide.

External RADIUS server

AlliedWare Plus can use an external RADIUS server, such as a FreeRADIUS server running in a Linux-based system.

Here are the basic steps and associated commands:

1. Set the remote RADIUS server hostname or IP address and key

awplus(config)# radius-server host {<hostname>|<ip-address>} key <string>

2. Set the Download Portal to use RADIUS group for authentication

awplus(config)# aaa authentication download-portal default group radius

- Note: If the **aaa authentication download-portal** command is not set, the Download Portal will attempt to authenticate users against the local user database._
- It is not recommended that Download Portal users be added to the local user database, as this would allow them to log into the device CLI and GUI.
- It is recommended that the Local RADIUS Server or a remote RADIUS or LDAP server be used for Download Portal authentication.

For more information about how to configure the external RADIUS server and to use the RADIUS server over TLS, see the RADIUS Feature Overview and Configuration Guide.

Configuring a firewall

In this section we create a custom application named 'dlp' with TCP as the protocol and a destination port to match the secure-listen port. Then we create entities to represent the Download Portal users and an entity to represent the Download Portal.

1. Create an application for Download Portal

The custom application should match the secure-listen port. In this example, that is port 443:

```
awplus(config)# application dlp
awplus(config-application)# protocol tcp
awplus(config-application)# dport 443
```

2. Create entities

One or more network entities are needed to represent the Download Portal Users. These should be as specific as possible to limit access. However, in the case where users are on the Internet this may need to be quite broad:

```
awplus(config)# zone public
awplus(config-zone)# network internet
awplus(config-network)# ip subnet 0.0.0.0/0
```

Another host entity represents the Download Portal, matching the secure-listen address:

```
awplus(config)# zone public
awplus(config-zone)# network public_int
awplus(config-network)# ip subnet 10.0.0.0/24
awplus(config-network)# host dlp
awplus(config-host)# ip address 10.0.0.1
```

3. Add a firewall rule

This rule allows traffic to reach the Download Portal:

```
awplus(config)# firewall
awplus(config-firewall)# rule permit dlp from public.internet to
public.public_int.dlp
```

Note: We recommend that firewall rules are configured to ensure that the Download Portal is only reachable by clients that you expect.

Configuring an HTTP trustpoint

By default, HTTP uses the 'default-selfsigned' trustpoint. With this configuration, clients accessing the Download Portal receive a browser warning about a self-signed certificate, potentially alarming the user. To address this issue, it is possible to configure an HTTP trustpoint that utilizes a certificate signed by a PKI, eliminating browser warnings for the clients and giving them confidence they are connecting to the device securely.

Before using the HTTP trustpoint command you will need to establish a trustpoint. You can create a local self-signed trustpoint using the example procedure outlined below.

1. Create a self-signed trustpoint

See the Public Key Infrastructure (PKI) Feature Overview and Configuration Guide.

2. Configure HTTP to use the trustpoint

```
awplus# configure terminal
awplus(config)# http trustpoint <your-trustpoint-name>
```

Setting up the Download Portal using the Device GUI

In this section, we'll walk you through the process of setting up and configuring the Download Portal using the Device GUI.

It includes:

- Create separate IP address/port pairs for the Device GUI and the Download Portal" on page 10
- "Adding resources for clients to access on the Download Portal" on page 11
- "Create users who can access the Download Portal" on page 14
- "Checking the Download Portal configuration" on page 16
- Creating firewall rules for exclusive Download Portal user access" on page 17
- "How to see the HTTP and HTTPS settings" on page 19

Create separate IP address/port pairs for the Device GUI and the Download Portal

- 1. Login to the Device GUI and go to System > Services.
- 2. In the **HTTPS Listening Addresses** section, add an IP address/port pair for accessing the Device GUI.
- 3. In the **HTTP/S Services** section, disable HTTP Port and HTTPS Port. This results in the loss-ofconnection warning.

Do it in this order, otherwise you will be unable to access the Device GUI. If you do find yourself unable to access the Device GUI, you can use the CLI to complete the configuration.

	🚺 Allied Telesi	is	AR3050S					awplus	Up time: 13 days 20:33	💄 manager	B Save
æ	Dashboard			N 4							A
*	Wizard 🗸	/	Service	Mana	gement						
Ø	Vista Manager mini 🛛 🗸	/							- 1		
â	Security ~	/	Services								-1
Ŀ	Licensed Features	/	Telnet		Enabled						
۲	Network Infrastructure 🗸	-	HTTP/S Services							🔹 Confi	gure
۲	Network Services	/	Name			Port					
-	User Management		HTTP Port		Disabled	none					
٠	System 1	`	HTTPS Port	3	Disabled	none					
	File Management										- 1
	License Management		HTTP Listening Add	iresses						+ Add Li	sten
	Services		Address —				Port —				
		2									_
	Logging		HTTPS Listening A	idresses						+ Add Secure Li	sten
	Trigger		Address —			Port -					
			10.00.00			443				Tel	ete

4. Go to Network Services > Download Portal.

In the HTTPS Listening Addresses section, add an IP address/port pair for the Download Portal.

-	Allied Telesis	AR3050S			awplus	Up time: 13 days 20:41	💄 manager	Save
æ	Dashboard							-
*	Wizard 🗸	Download Porta	I				🔅 Ena	abled
0	Vista Manager mini 🛛 🗸							_
â	Security 🗸	HTTPS Listening Addresses					+ Add Secure L	isten
0	Licensed Features 🗸 🗸	Address —		Port -				
⊕	Network Infrastructure \lor	100.000-00		443			T De	lete
⊜	Network Services	10.00.00		10443			T De	lete
	DHCP Server							
	SMTP Server	Resources				+ Add Li	nk + Add Reso	ource
	Tools	Path	Description		Digest - SHA256			
	RADIUS							-
	AAA	/flash/vpn_client.ovpn	client openvpn config			Vi	ew Detail 👔 De	lete
	SNMP	https://upusu.elliadtelesis.com	annany wahaita					
	Download Portal	nttps://www.aiiiedtelesis.com	company website			Vi	ew Detail 📋 De	lete

Adding resources for clients to access on the Download Portal

Within this section of the guide, we will focus specifically on the work-flow of adding resources to the Download Portal using the Device GUI. These are the resources hosted on the device that will be displayed in the Download Portal page.

- 1. Go to System > File Management
- 2. Click the **Upload** button. Navigate to where the file is stored, and confirm the upload.
- 3. The file is now displayed in the File Management window.

	Allied Telesis	AR3050S				awplus	Up time: 14 days 22:12	💄 manager	Save
@ *	Dashboard Wizard v	File Management						S Rei	boot
0	Vista Manager mini 🗸	/fs /flash			2	Set Boot R	elease File		
C	Licensed Features V	Name ~	Modified — 1/31/2024, 3:19:21 PM	Size(bytes) - 12	Actions	Current: Backup:	Not Set	Brov	NSP
₿	Network Infrastructure v Network Services v	tools	3/11/2024, 3:47:50 PM			Set Boot C	onfig File		
-	User Management	e opentext.cfg	7/24/2023, 2:44:34 PM	3190	ODownload Delete	Current:	flash:/dlp.cfg	Brow	vse
•	About 1	offload gui-userdata	8/3/2020, 12:57:21 PM 3/1/2022, 1:14:22 PM			Backup: Running:	Not Set	D View Configurat	vse
	File Management License Management Services	gateway.cfg	4/19/2022, 3:32:17 PM	2563	O Download	Flash Usag	je		
	SSH Time	dip.cfg	2/26/2024, 1:31:14 PM	2702	O Download Delete	11%		381.3M / 3.6	iG
	Logging Trigger	default.cfg backup.cfg	5/24/2022, 10:22:49 AM 10/13/2020, 11:31:18 AM	723	Download Delete Delete				
	CLI 🗹		2/16/2024 11:10:47 AM	4501504					

- 4. Go to Network Services > Download Portal
- 5. Click +Add Resource

	Allied Teles	Sis	AR3050S			awplus	Up time: 13 days 21:13	💄 manager	🔒 Save				
A	Dashboard												
*	Wizard	~	Download Porta					🗢 Disa	bled				
0	Vista Manager mini	~											
Ĥ	Security	~	HTTPS Listening Addresses					+ Add Secure Li	sten				
C	Licensed Features	~	Address —		Port -								
۲	Network Infrastructure	~	102.000.000		443			T De	lete				
۵	Network Services	~	10.00		10443			1 De	lete				
	DHCP Server							5					
	SMTP Server		Resources				+ Add L	ink + Add Reso	urce				
	Tools		Path	Description		Digest - SHA256							
	AAA		/flash/vpn_client.ovpn	client openvpn config			v	iew Detail 📋 De	lete				
	SNMP Download Portal		https://www.alliedtelesis.com	company website			٧	iew Detail 📋 De	lete				

- 6. Select a resource from the drop-down list.
- 7. In the Add Resource window, add a Description and Digest SHA265 (data integrity check).
- 8. Click Apply.

Add Resource	6
Resource	flash:/vpn_client_conf.ovpn
Description	
OpenVPN client configuration file	
Digest - SHA256	
e3b0c44298fc1c149afbf4c8996fb92427ae41e464	19b934ca495991b7852b855
	Cancel Apply

9. The resource is now visible in the Download Portal.

	Allied Telesis	AR3050S			awplus	Up time: 2 days 22:53	💄 manager	Save
a a *	Dashboard Wizard ~	Download Po	ortal				🖨 Dis	abled
© 8	Vista Manager mini v Security v	HTTPS Listening Addresses					+ Add Secure L	isten
C	Licensed Features 🗸 🗸	Address —		Port				_
•	Network Infrastructure V	102.108.118		443			The De	lete
	DHCP Server SMTP Server	Resources				+ Add L	ink + Add Reso	burce
	Tools RADIUS	Path	Description	Digest - SHA256				
	AAA SNMP	/flash/vpn_client_conf.ovpn	OpenVPN client configuration file	e3b0c44298fc1c149afbf4c8996fb92427ae41e	4649b934ca49599	91b7852b855	riew Detail 📋 De	lete
	Download Portal	https://alliedtelesis.com	Company website			N	riew Detail 🔋 De	lete

	Allied Telesis	AR3050S		awplus	Up time: Error getting up time	💄 manager	B Save
m *	Dashboard Wizard v	Download F	Portal		10 —	Dise	and
\$	Vista Manager mini v	HTTPS Listening Addresses				+ Add Secure L	isten
C	Licensed Features 🗸	Address —		Port —			
()	Network Infrastructure 🗸	Resources			+ Add L	ink + Add Reso	purce
۲		Path	Description	Diges	t - SHA256		
	DHCP Server SMTP Server Tools RADIUS AAA SNMP Download Portal						
	User Management						

Click **Restart**. This is necessary so the Download Portal settings can be applied.

Downlo	oad Portal		C Disabled
	Enable the Download Portal	×	
HTTPS Listenin	This will restart the web server and GUI users will be longed out		+ Add Secure Listen
Address —			
Resources		Cancel Restart	+ Add Link + Add Resource
Path	Description	Digest - SHA	256

Create users who can access the Download Portal

This section describes how use the Device GUI to create Download Portal users using a **Local** RADIUS server. For information on setting up an <u>external</u> RADIUS server, please see the RADIUS Feature Overview and Configuration Guide.

Download Portal users are authenticated using the AAA authentication service. The authentication group can use RADIUS or LDAP. For information on LDAP, see the LDAP Feature Overview and Configuration Guide.

To create a new Download Portal user:

- 1. Go to Network Services > RADIUS
- 2. Turn on the RADIUS server.

When you turn on the RADIUS server, the NAS field will be automatically populated.

3. Click + New User

	Allied Tele	zsis [°]	AR3050S					awplus	Up time: 13 days 2	1:52	manager	🖥 Sav	ve
a *	Dashboard Wizard	~	Local	RADIUS S	Server					2	ом 🔫		•
0	Vista Manager mini	×:								Export	Local CA Cer	tificate	
ê	Security Licensed Features	× 	Users		🔥 Import	CSV 🚯 Export CSV	Groups		k	Import CSV	🚯 Export	CSV	
⊕	Network Infrastructur	e 🗸	User	Group		3 + New User	Group	VL	AN		+ New Gr	oup	
₿	Network Services	^	client1		▲ Export	🖍 Edit 🔋 Delete	NAS					2	
	DHCP Server						NAS	Key			+ New I	VAS	
							127.0.0.1	awplu	s-local-radius-server		Te De	lete	
	AAA SNMP												
	Download Portal												
-	User Management												
٠	System	~											*

4. Enter the username and password and click Apply.

Local	RADI	JS Server			
		New User	_	×	
Users		Username MyDLPUser			
User	Grou	Password Enter password			VLAN
		Group	None	~	
NAS		Can	cel 🛛	Apply	
NAS	Key	+ New NAS			

- 5. Go to Network Services > AAA
- 6. Click + New Host and enter the local RADIUS server IP address, key, authentication and accounting ports.



7. Configure the Download Portal to use the configured RADIUS server for authentication. **This** needs to be entered on the CLI.

For example:

awplus(config)# aaa authentication download-portal default group radius

- Note: If the **aaa authentication download-portal** command is not set, the Download Portal will attempt to authenticate users against the local user database.
- It is not recommended that Download Portal users be added to the local user database, as this would allow them to log into the device CLI and GUI.
- It is recommended that the Local RADIUS Server or a remote RADIUS or LDAP server be used for Download Portal authentication

Checking the Download Portal configuration

You can check the Download Portal configuration using the commands below:

```
awplus#show running-config download-portal
download-portal
uri https://alliedtelesis.com description Company website
file flash:/vpn_client_conf.ovpn sha256sum
e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855 description
OpenVPN client configuration file
secure-listen 10.33.25.35 10443
secure-listen 192.168.1.15 443
enable
!
```

awplus#show download-portal
Status: Enabled
Files: 2
Secure-listen Addresses:
10.33.25.35:10443
192.168.1.15:443
awplus#

Creating firewall rules for exclusive Download Portal user access

In this section we create a custom application named 'dlp' with TCP as the protocol and a destination port to match the secure-listen port. Then we create entities to represent the Download Portal users and an entity to represent the Download Portal.

1. Create an application for the Download Portal

Go to Security > Applications

• The custom application should match the secure-listen port.

	Allied Telesis	AR3050S			awplus	Up time: 13 days 23:45	💄 manager	Save
@a *	Dashboard Wizard v	Applications				DP	disabled	
© 8	Vista Manager mini v	Applications are used when creating Firewall, NAT Enable DPI (Deep Packet Inspection) to provide au here to manage the licensed Procera application li You may also create custom applications that will	and Traffic Contr tomatic applicationst.	ol rules. on identification. Alternatively, th	ne large Procera application library will be ava	ilable if the Application Control	license is enable	d. Click
	Entities Applications Firewall NAT	Custom Applications	be used in preters	ence to or r appreations below.				
	Traffic Control	Name	Protocol			+	New Custom Applic	ation
	Custom URL Filtering	dip	TCP	Source Port:	Destination Port: 10443		🖍 Edit 📋 🕻	elete
C	Licensed Features 🗸							
•	Network Infrastructure 🗸							
•	Network Services							

2. Create entities

Go to Security > Entities

- One or more network entities are needed to represent the **Download Portal users**. These should be as specific as possible to limit access.
- Create another entity to represent the **Download Portal**, matching the secure-listen address.

	Allied Telesis	AR3050S	awplus	Up time: 13 days 23:37	💄 manager	B Save
æ	Dashboard				_	^
*	Wizard 🗸 🗸	Entity Management				
S	Vista Manager mini 🔍	3 Zones 5 Networks 4 Hosts			+ Nev	Zone
ê	Security ^					
	Entities	C openvpn_routes	2 pul	blic	1	Edit
	Applications	2 Networks + New Network 1 Network + New Network	2 Netwo	orks	+ New Netw	ork
	Firewall	🔕 internet 1 Host 🕨 🔕 Ian 1 Host 🕨	N inte	ernet	0 Hosts	•
	NAT Traffic Control	🚺 local 1 Host 🕨	N pul	olic_int	1 Host	•
	Intrusion Prevention					

3. Add a firewall rule

Go to Security > Firewall

1	Allied Telesis	1	AR3050S					awplus	Up time: 14 days	00:04	💄 manager	Save
a a *	Dashboard Wizard v	*	Firewall								OFF	ĥ
8	Vista Manager mini 🔍	3	Rules							Export	To Csv + Nev	v Rule
-	Security ^		Firewall Rules							Filter		
	Applications		Action	Application	From	То	Errors					
	Firewall NAT		Permit	https	² private	Bprivate / lan / lan_int				1	Edit 📋 Delete	
	Traffic Control											
	Custom URL Filtering											
C	Licensed Features 🗸											
۲	Network Infrastructure 🗸											
۲	Network Services											
	DHCP Server											
	SMTP Server	*										v

- Click + New Rule
- Select an Action, Application, From, To, and click Apply

Edit Firewall Rule		×
Action	Permit	~
Application https https		
From	public / internet	~
То	public / public_int / dlp	~
	Cancel	pply

We recommend that firewall rules are configured to ensure that the Download Portal is only reachable by clients that you expect.

How to see the HTTP and HTTPS settings

Go to **System** > **Services** to see the HTTP and HTTPS settings configured on the device.

	🔀 Allied Tele	sis	AR3050S			awplus	Up time: 14 days 00:58	💄 manager	Save
A	Dashboard		Sorvice Mone	acomont					*
*	Wizard	~	Service Maria	gement					
0	Vista Manager mini	~							_
e	Security	~	Services						
C	Licensed Features	~	Telnet	Disabled					
۲	Network Infrastructure	~	HTTP/S Services					🏚 Confi	gure
۲	Network Services	~	Name		Port				
	User Management		HTTP Port	Disabled	none				
٠	System	^	HTTPS Port	Disabled	none				
	About File Management								
	License Management	H	HTTP Listening Addresses					+ Add Li	sten
	Services		Address —			Port —			
			HTTPS Listening Addresses					+ Add Secure Li	sten
	Trigger		Address —		Port —				
			10.33.25.35		443			T Del	ete

How do users access the Download Portal?

The Download Portal administrator provides the Download Portal user with:

- A link to the Download Portal, which is either the IP/port configured as the secure-listen address, or FQDN name that points to that IP address.
- Instructions for logging in to the Download Portal.
- Additional information about available resources can also be provided as needed.

Download Portal	
Username	
User1	
Password	
•••••	
	Sign in

ownload Portal		
Welcome to the Download Portal.		
Software & Configuration Downlo	pad	
OpenVPN client configuration file	vpn_client_conf.ovpn	Download
Bookmarks		

C613-22143-00-REV A

Allied Telesis

NETWORK SMARTER

 North America Headquarters
 19800 North Creek Parkway
 Suite 100
 Bothell
 WA 98011
 USA
 T: +1
 800 424 4284
 F: +1
 425 481 3895

 Asia-Pacific Headquarters
 11 Tai Seng Link
 Singapore
 534182
 T: +65 6383 3832
 F: +65 6383 3830

 EMEA & CSA Operations
 Incheonweg 7
 1437 EK Rozenburg
 The Netherlands
 T: +31 20 7950020
 F: +31 20 7950021

© 2024 Allied Telesis, Inc. All rights reserved. Information in this document is subject to change without notice. All company names, logos, and product designs that are trademarks or registered trademarks are the property of their respective owners.