

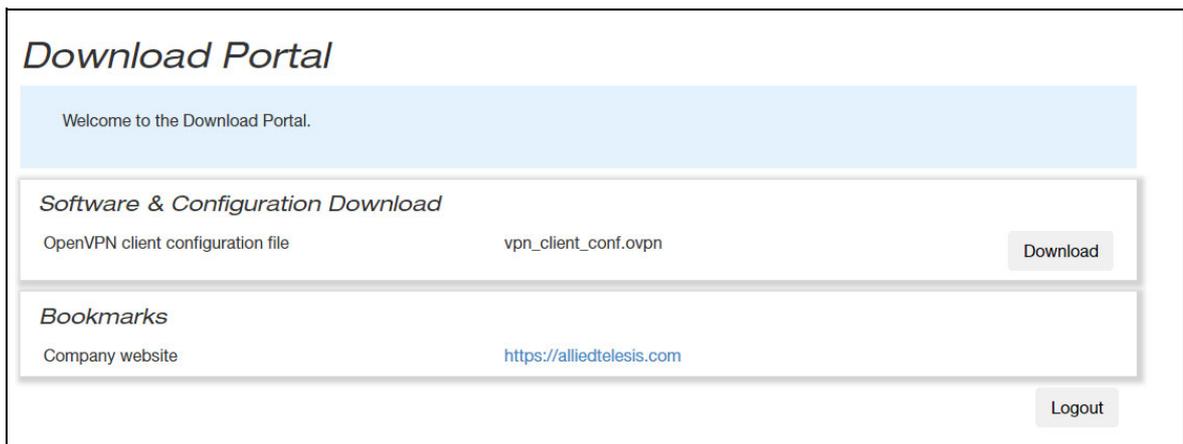
Download Portal

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:



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 GUI	10
Create separate IP address/port pairs for the Device GUI and the Download Portal	10
Adding resources for clients to access on the Download Portal.....	11
Create users who can access the Download Portal	14
Checking the Download Portal configuration	16
Creating firewall rules for exclusive Download Portal user access	17
How to see the HTTP and HTTPS settings.....	19
How do users access the Download Portal?	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 a1bed1569bef6b9f8958bf8993ef53bf7c2f62a1833fe41f14
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 secure-listen 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.

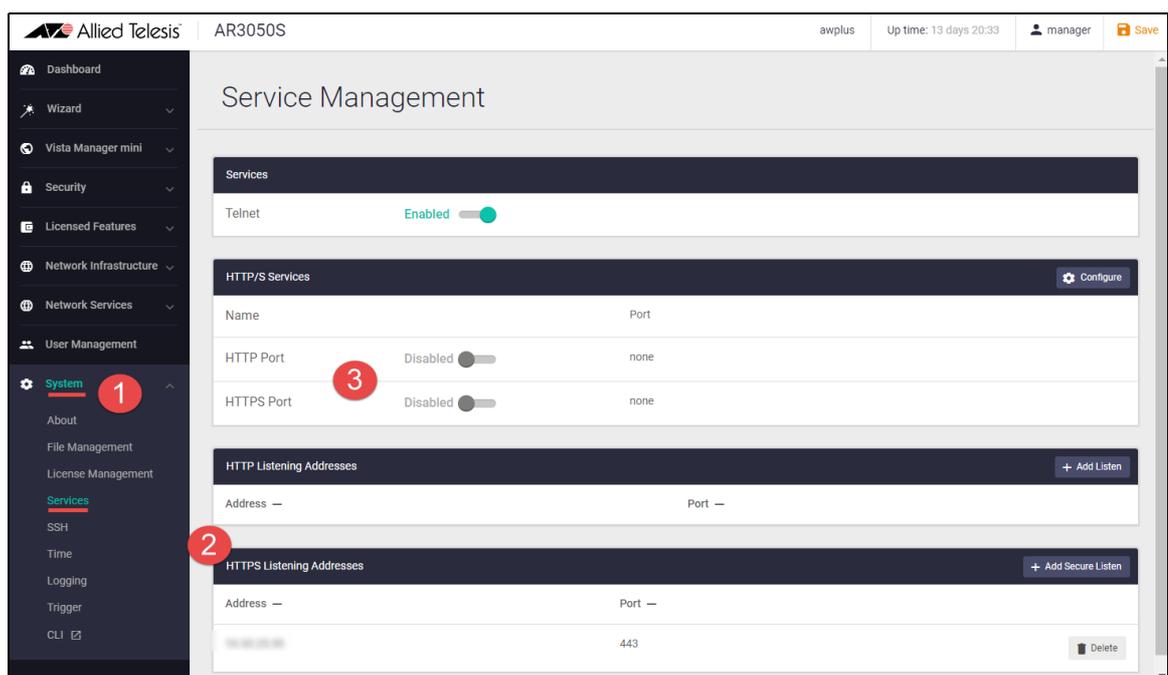
It includes:

- "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-of-connection 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.



4. Go to **Network Services > Download Portal**.

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

The screenshot shows the 'Download Portal' configuration page. The 'HTTPS Listening Addresses' section is highlighted with a red box and a red circle containing the number '4'. The table below it lists the following addresses and ports:

Address	Port	Action
192.168.1.10	443	Delete
192.168.1.10	10443	Delete

Below the listening addresses is the 'Resources' section, which contains a table of resources:

Path	Description	Digest - SHA256	Action
/flash/vpn_client.ovpn	client openvpn config		View Detail, Delete
https://www.alliedtelesis.com	company website		View Detail, Delete

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.

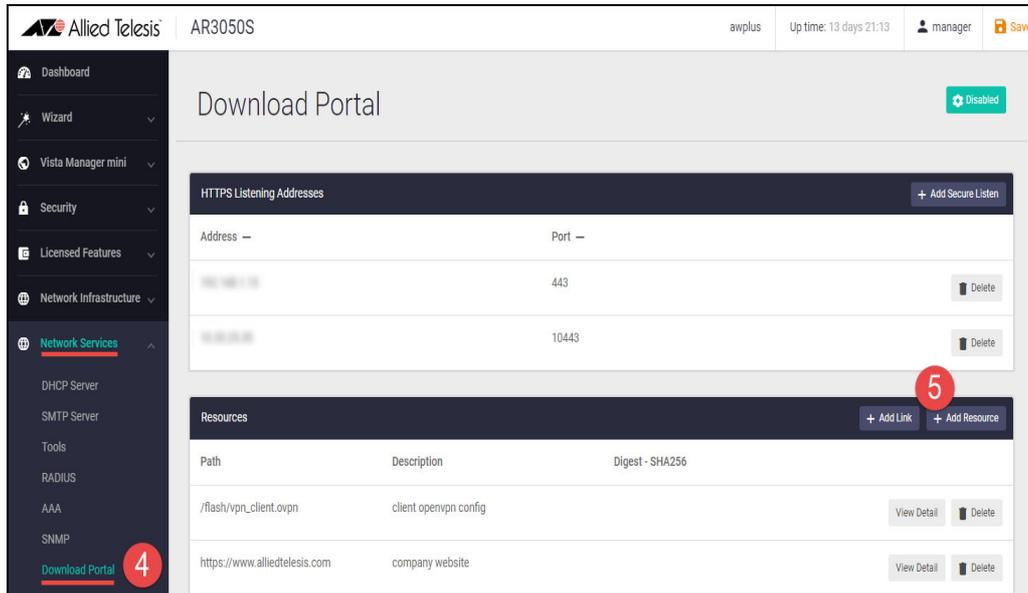
1. Go to **System > File Management**
2. Click the **Upload** button. Navigate to where the file is stored, and confirm the upload.
3. The file is now displayed in the File Management window.

The screenshot shows the 'File Management' page. The 'System' menu item is highlighted with a red circle and the number '1'. The 'Upload' button is highlighted with a red circle and the number '2'. The file 'opentext.cfg' is highlighted with a red circle and the number '3'. The file list is as follows:

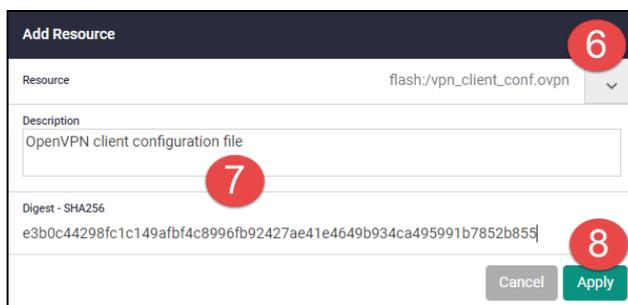
Name	Modified	Size(bytes)	Actions
vpn_client.ovpn	1/31/2024, 3:19:21 PM	12	Download, Delete
tools	3/11/2024, 3:47:50 PM		
opentext.cfg	7/24/2023, 2:44:34 PM	3190	Download, Delete
offload	8/3/2020, 12:57:21 PM		
gui-userdata	3/1/2022, 1:14:22 PM		
gateway.cfg	4/19/2022, 3:32:17 PM	2563	Download, Delete
dip.cfg	2/26/2024, 1:31:14 PM	2702	Download, Delete
default.cfg	5/24/2022, 10:22:49 AM	723	Download, Delete
backup.cfg	10/13/2020, 11:31:18 AM	786	Download, Delete

On the right side, there are sections for 'Set Boot Release File', 'Set Boot Config File', and 'Flash Usage'.

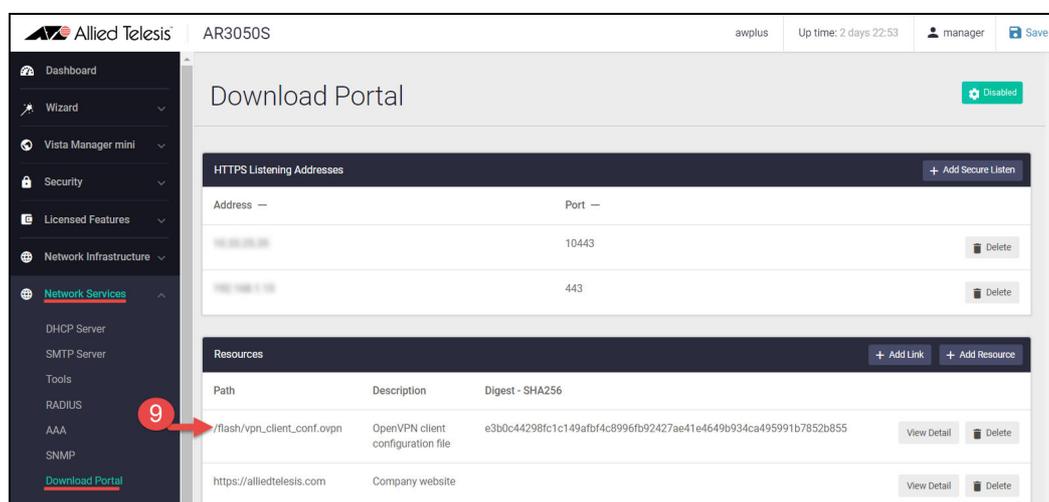
4. Go to **Network Services > Download Portal**
5. Click **+Add Resource**



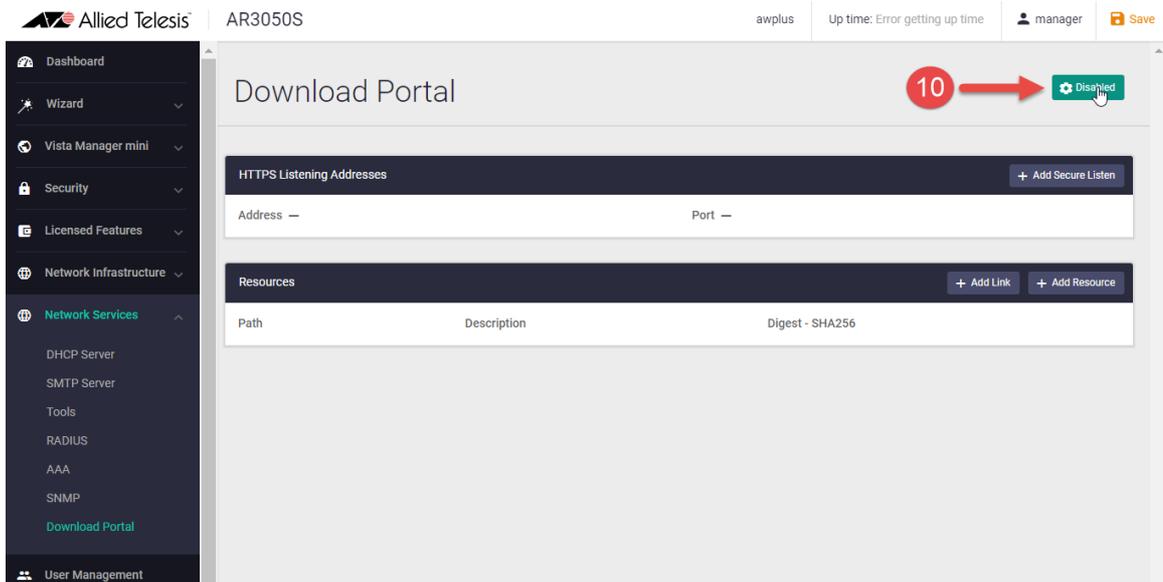
6. Select a resource from the drop-down list.
7. In the **Add Resource** window, add a **Description** and **Digest - SHA256** (data integrity check).
8. Click **Apply**.



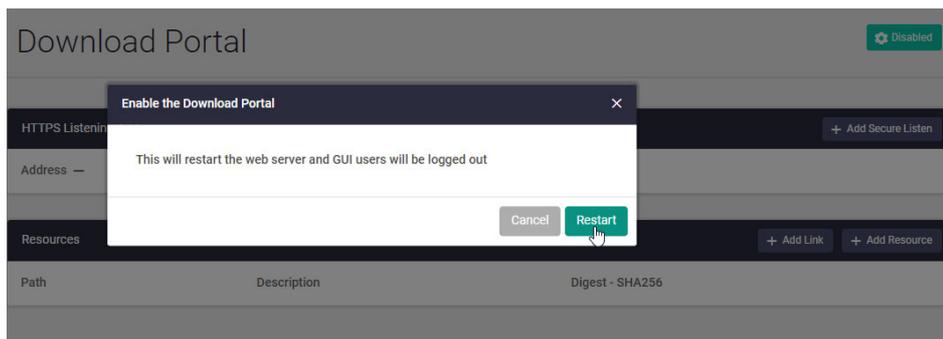
9. The resource is now visible in the Download Portal.



10. Enable Download Portal - Go to **Network Services > Download Portal** and click **Disabled**



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



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 external RADIUS server, please see the [RADIUS Feature Overview and Configuration Guide](#).

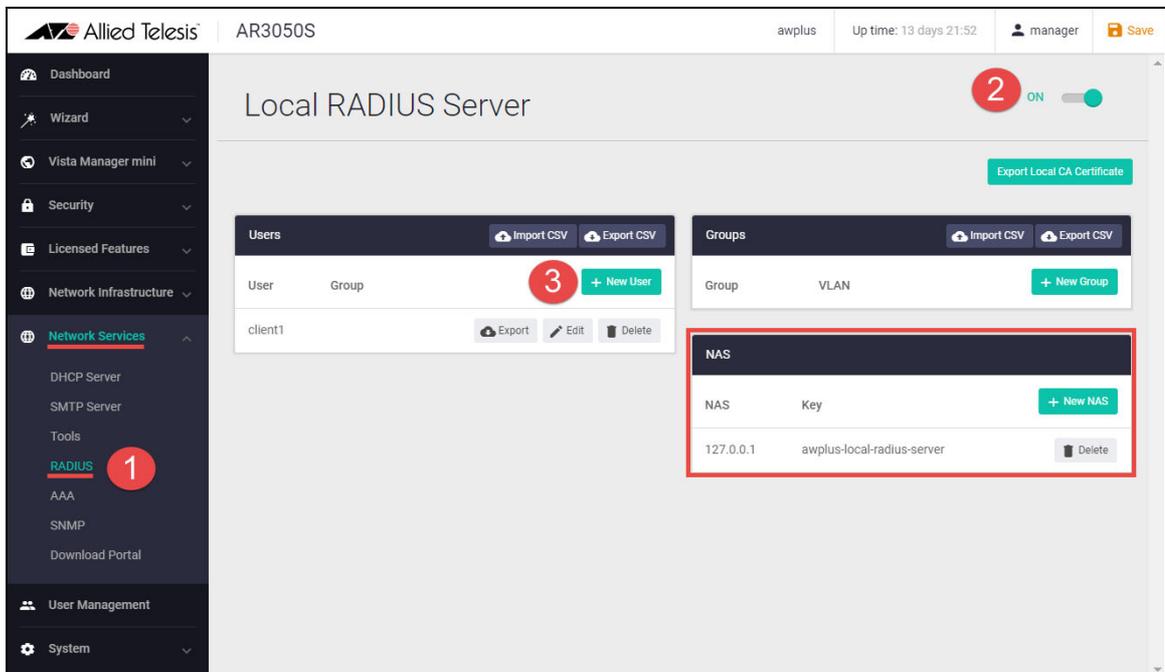
Download Portal users are authenticated using the AAA authentication service. The authentication group can use RADIUS or LDAP. For information on LDAP, see the [LDAP Feature Overview and Configuration Guide](#).

To create a new Download Portal user:

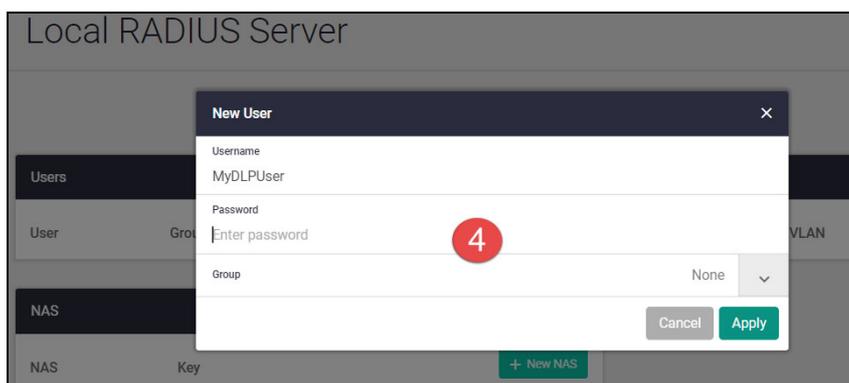
1. Go to **Network Services > RADIUS**
2. Turn on the RADIUS server.

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

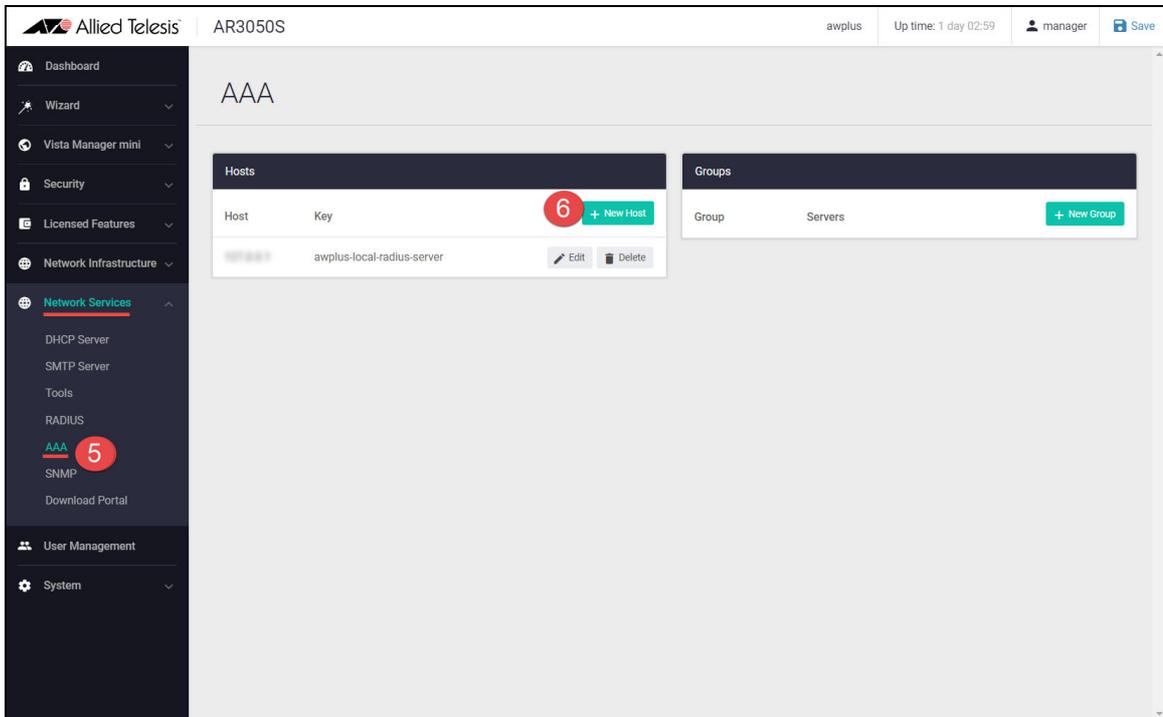
3. Click **+ New User**



4. Enter the username and password and click **Apply**.



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
e3b0c44298fc1c149afb4c8996fb92427ae41e4649b934ca495991b7852b855 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#
```

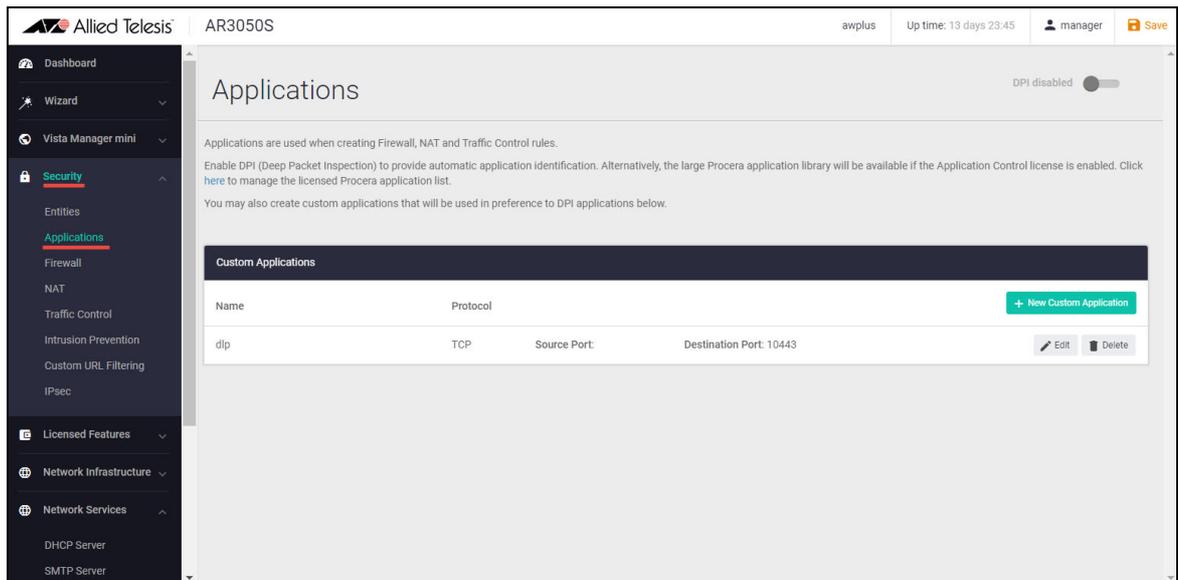
Creating firewall rules for exclusive Download Portal user access

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**

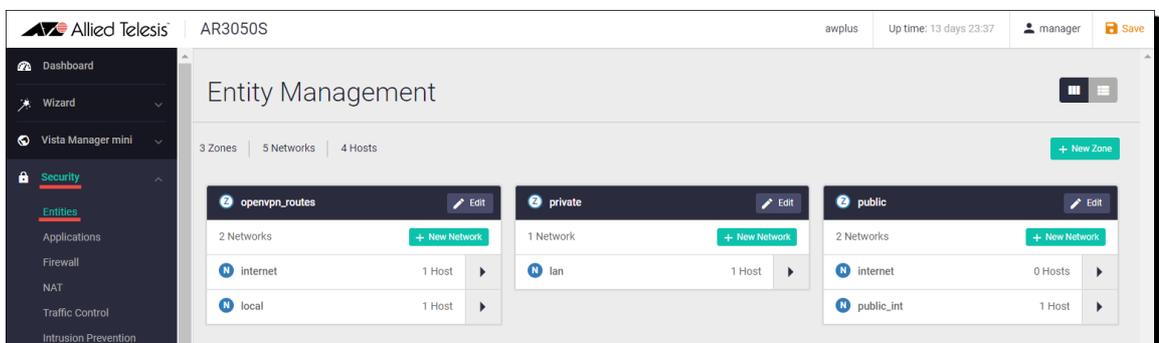
- The custom application should match the secure-listen port.



2. Create entities

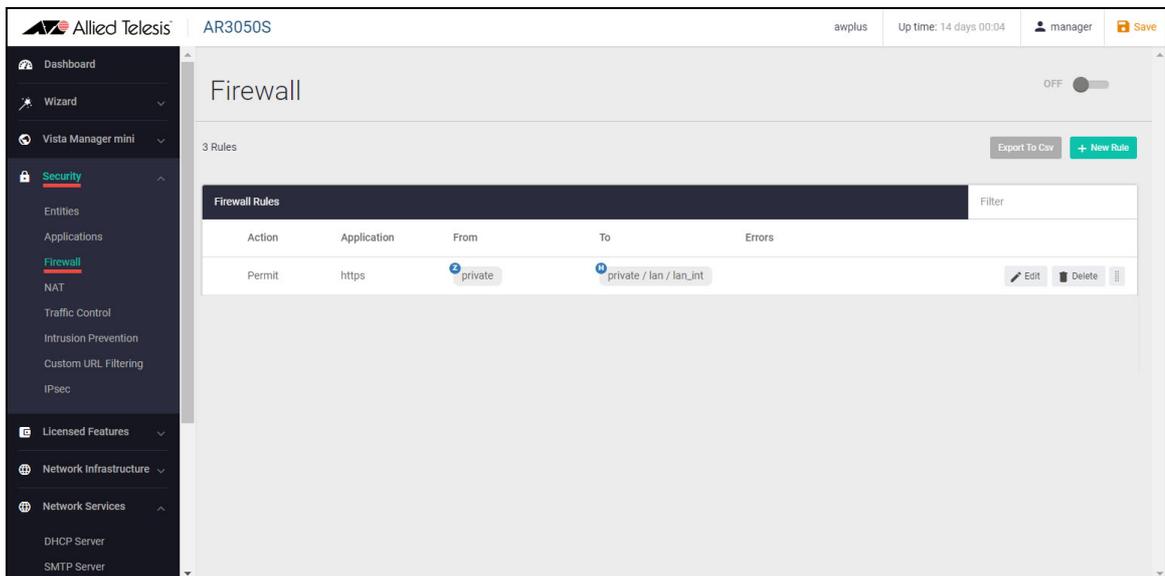
Go to **Security > Entities**

- 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.



3. Add a firewall rule

Go to **Security > Firewall**



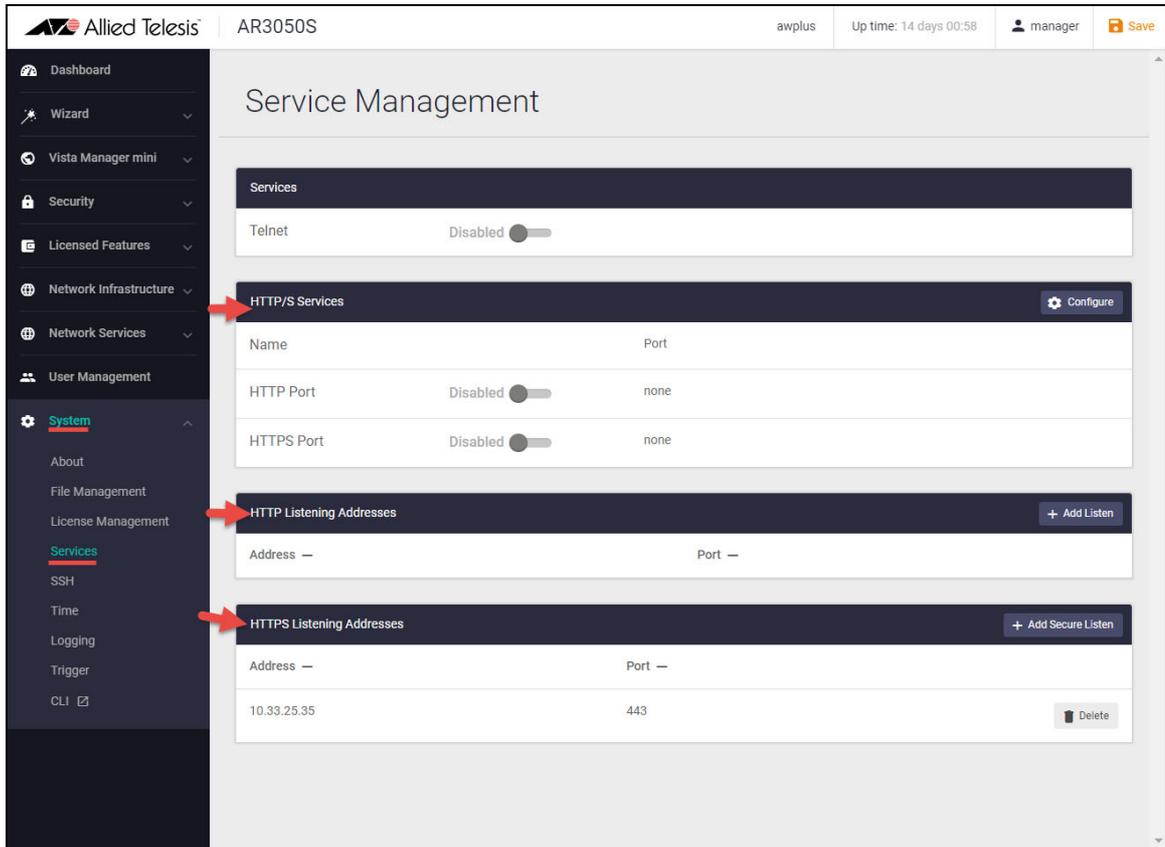
- Click **+ New Rule**
- Select an Action, Application, From, To, and click **Apply**

Action	Permit
Application	https
From	public / internet
To	public / public_int / dlp

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.



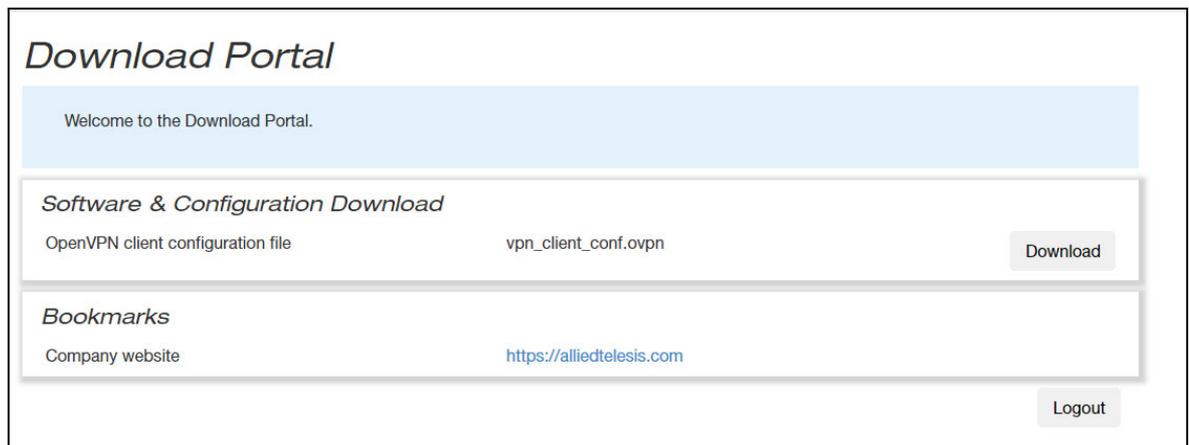
How do users access the Download Portal?

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.



The screenshot shows the login interface for the Download Portal. It features the title "Download Portal" at the top. Below the title are two input fields: "Username" with the text "User1" and "Password" with masked characters "*****". A "Sign in" button is located at the bottom right of the form.



The screenshot shows the home page of the Download Portal. It features the title "Download Portal" at the top. Below the title is a light blue banner with the text "Welcome to the Download Portal." Underneath the banner are two main sections. The first section is titled "Software & Configuration Download" and contains a table with two columns: "OpenVPN client configuration file" and "vpn_client_conf.ovpn". A "Download" button is located to the right of the second column. The second section is titled "Bookmarks" and contains a table with two columns: "Company website" and "https://alliedtelesिस.com". A "Logout" button is located at the bottom right of the page.

C613-22143-00-REV A



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

alliedtelesिस.com

© 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.