Awingu
Admin Manual

Version 5.2

Document Guidance

Introduction	This document is an introduction to the Awingu Admin Guide which provides guidelines for integrators and customer system administrators for operating a Awingu environment.
Related Documents	*Awingu User Manual 5.2*
Feedback	We strive to continuously improve our products and to develop solutions that fit the needs of our customers. For questions or feedback on this document, please contact: **feedback@awingu.com**
Last Updated	11/10/2021
Contact Details	**Awingu N.V.** Ottergemsesteenweg-Zuid 808, B44 9000 Gent Belgium Telephone:+32 (0) 9 296 40 11
Intended Audience	This guide is intended for Awingu integrators and system administrators.
Confidentiality/Disclaimer	All rights in and title to this document and all information contained and referenced within are owned by Awingu and its licensors unless expressly stipulated otherwise. This document is issued in confidence and must not be reproduced in whole or in part or given or communicated to any third party without the prior written consent of Awingu. It may not be used except for the restricted purpose for which it is made available to you. Awingu does not warrant that the information contained and referenced herein is accurate or complete, and nothing herein constitutes investment, tax, legal or other advice, nor should it be relied on in making an investment or other decision. Awingu shall not be liable for any loss, expense, damage or claim arising from the statements made or omitted to be made, or advice given or omitted to be given in this document.

Installation

Introduction

This guide describes how you can install and deploy the Awingu virtual machine.

- Connectivity Requirements
- Sizing & Scaling Requirements
- Deployment
- Awingu Installer
- Azure Awingu All-In-One

Connectivity Requirements

Introduction

Before starting a deployment of the Awingu platform, a few connectivity requirements needs to be checked and/or enabled. Please review this section to ensure proper installation and operation.

Connectivity Requirements during Installation:

During installation of the Awingu appliance as virtual machine (VM), we need to be able to have a connection to Awingu's repository servers and sync to the right time-zone.

Connection	From	To
NTP: UDP port 123	The Awingu-VM	On- or off-site NTP service. A common use case it to use the NTP service of the AD service. The NTP service should use the same time zone as the hypervisor (UTC is recommended).
DNS: UDP port 53	The Awingu-VM	DNS server which resolves the NTP (when provided via FQDN*) and Awingu's repository servers (repo-pub.awingu.com). A common use case it to use the DNS service of the AD service.
HTTP : TCP port 8080	The browser of the operator	The Awingu-VM
HTTP : TCP port 80	The browser of the operator	The Awingu-VM

* FQDN = Fully Qualified Domain Name, e.g. ntp.mycompany.com

Connectivity Requirements during Operation and Configuration:

The Awingu appliance has a few requirements for correct operation. Before deployment, check whether the following ports can be opened.

Connection	From	To
LDAP(s): TCP port 389 (or TCP port 636 for SSL encryption)	The Awingu-VM	LDAP or Active Directory server(s) back-end
KERBEROS: UDP/TCP port 88 and TCP port 464	The Awingu-VM	Kerberos server (Only required when users need to be able to change password at next logon) The kerberos server should also have PTR (reverse DNS) and SRV records in place to locate the KDC server and define the protocol to use**
RADIUS (if used): UDP port 1812	The Awingu-VM	RADIUS service for second factor authentication
CIFS (if used): UDP port 137, TCP port 445	The Awingu-VM	CIFS/SMB file server(s) back-end
WebDAV (if used): TCP port 80 or 443 (or different depending on WebDAV config)	The Awingu-VM	WebDAV file server(s) back-end
RDP: TCP port 3389 (RDP /RemoteApp)	The Awingu-VM	To application server(s) back-end
NTP: UDP port 123	The Awingu-VM	On- or off-site NTP service. A common use case it to use the NTP service of the AD service.

HTTPS: TCP port 443	The Awingu-VM	• Awingu's repository servers: https://repo-pub.awingu.com (directly or via the configured HTTP proxy - see Connectivity Settings). Only mandatory during upgrades, but required for Anonymous Usage Reporting. • When using SaaS services, those services need to be reachable by Awingu or via the configured HTTP proxy (see Connectivity Settings): • Microsoft OneDrive for Business: • <mydmain>**-my**.sharepoint.com • login.microsoftonline.com • graph.microsoft.com • DUO Multi-Factor Authentication: • <your_api>.duosecurity.com • Automatic certificates through Let's Encrypt (see Certificate Settings): • *.api.letsencrypt.org (⚠ only directly, not through HTTP proxy)
HTTP(S): TCP port 80/443	The Awingu-VM	Web applications reversed proxied by Awingu
DNS: UDP port 53	The Awingu-VM	DNS server which resolves all connections mentioned above (when provided as FQDN*)
HTTP: TCP port 80 (long living WebSocket)	The (end user browser) client***	• The Awingu-VM • When using automatic certificates (see Certificate Settings): the servers of Let's Encrypt
HTTPS: TCP port 443 (long living WebSocket)	The (end user browser) client***	• The Awingu-VM (Only when SSL Offloader enabled in Connectivity section) • When using automatic certificates (see Certificate Settings): the servers of Let's Encrypt
SNMP (if used): UDP port 161	Monitoring System	The Awingu-VM (Only if SNMP enabled in Connectivity section)
HTTP(s) : TCP port 80/443	All servers involved in Kerberos Authentication (AD and Application Servers)	The-Awingu-VM (http(s)://<AWINGU_URL>/crl/<AWINGU_DOMAIN_NAME>)

* FQDN = Fully Qualified Domain Name, e.g. ntp.mycompany.com
** e.g. *kerberos-master.*(tcp|udp).staging.awingu.com - For more information: https://technet.microsoft.com/en-us/library/cc961719.aspx
*** When this connections goes via an SSL-offloader, reverse proxy, firewalls, etc., please make sure that WebSockets are supported and that open WebSocket connections are not killed after a while. See SSL offloader, reverse proxy or loadbalancer settings for other important settings.

⚠ For **multi node** deployment, all TCP, UDP and ICMP traffic should be allowed between the nodes. This traffic is not encrypted. Each node has an internal firewall only allowing traffic from other nodes (based on the IP address).

ℹ Version 4.2 added support for accessing Awingu via an other port than 80 or 443. E.g. https://awingu.company.com:81

Note: Using Awingu as an IDP in combination with accessing Awingu via an other port than 80 or 443 is not tested.

Sizing & Scaling Requirements

Standard (minimum) setup

for a standard single node setup the minimum sizing requirements are:

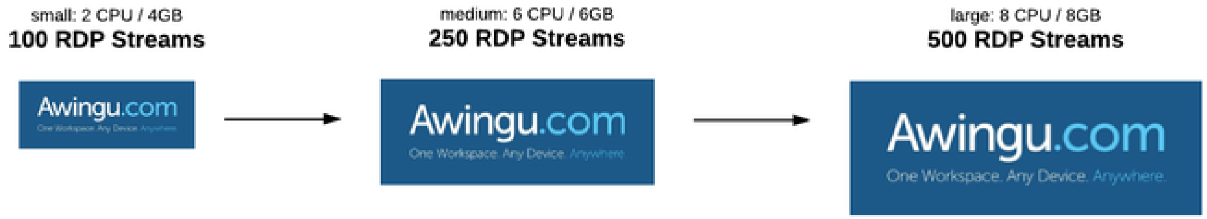
- 2 vCPU's
- 4 GB of memory
- 80 GB of diskspace

Scaling

An Awingu Setup can scale on 3 levels:

1) In the appliance

By adding more memory / CPU to a virtual appliance



When adding extra resources like CPU & Memory to an appliance, Awingu will be able to handle more RDP streams and file operations.

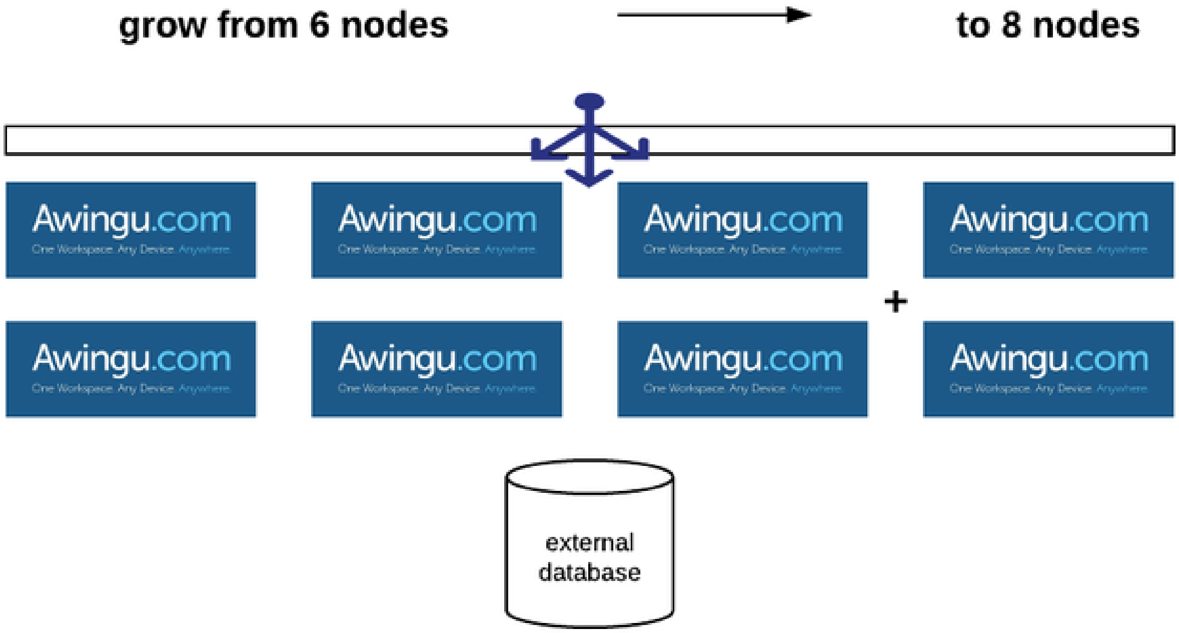
The 8 CPU / 8 GB is not a hard limit but in general we recommend for environments with more then 500 concurrent RDP streams to go to 3 medium servers rather then to grow the single node.

2) In the cluster

Awingu can be configured in multi node setup. See Service Management Settings for instructions how to do this. In such a setup multiple Awingu nodes form a cluster. By adding more nodes to the cluster you can scale out your Awingu setup. Adding extra nodes can be done at any time without service impact if the nodes are front-end only nodes.

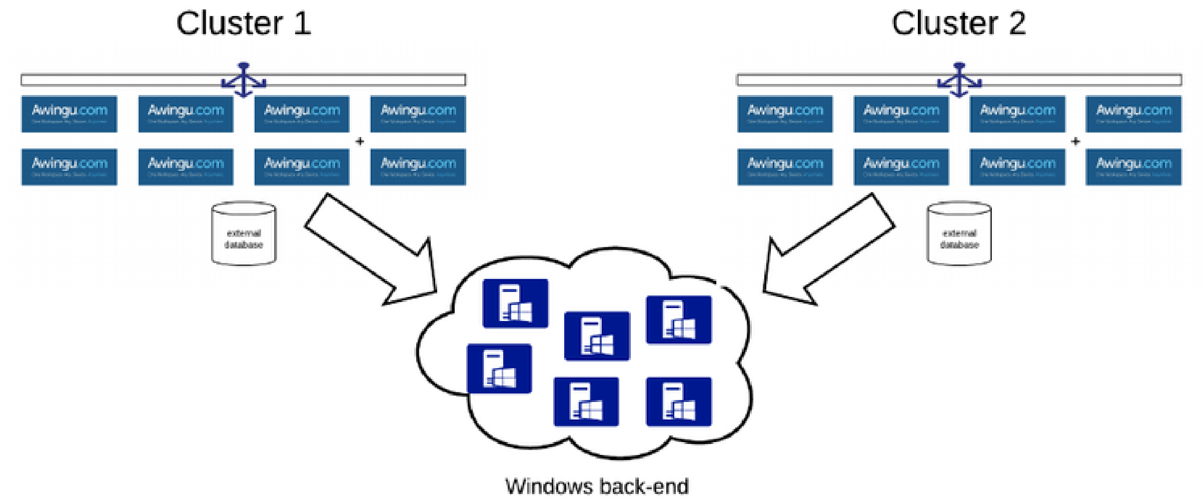
For this scenario Awingu assumes that all data is stored in an external database and that there is a loadbalancer in front of Awingu to load the incoming requests over the different Awingu virtual appliances.

For a cluster setup there is only 1 system settings and 1 dashboard so all changes are done automatically to all nodes of the cluster. When upgrading to a new version the full cluster will be upgraded at the same time.



3) Making multiple clusters pointing to the (same) Windows Backend

As there is no Awingu software on the Windows back-ends it is possible to have multiple, independent clusters pointing to the same windows back-end.



When going to multiple clusters the configuration of each cluster needs to be maintained separately. If needed this can be (partially) automated via the Awingu API. (See Automate Awingu via the REST API)

Sizing Parameters

The sizing of an Awingu environment is mainly determined by:

- The amount of concurrent RDP streams (number of RDP sessions going from the Awingu appliance to the windows backend(s))

- Type of RDP / Remote apps published behind Awingu (apps with lots of screen updates will require more resources then traditional business apps)
- The amount of concurrent file operations (generating previews and file shares)
- Size of the file operations (small files will require less resources then large files)

Next to this other factors may influence the Awingu sizing:

- CPU speed / Type
- Overall performance of the underlying storage system
- Overall load on the hypervisor
- High Availability (HA) requirements

For simplicity reasons we have mapped these parameters to 2 user profiles:

- **Light Concurrent User:** User that has 1 RDP stream open and does not use the file operations heavily. This is typically the case when publishing VDI's or when all remote apps in a collection are merged into a single RDP stream.
- **Heavy Concurrent User:** User that has 3 RDP streams open, 10 accesses to reverse proxied web applications and does a number of file operations per hour per user.

Also note that all recommendations are based on concurrent users. A concurrent user is a user that is logged in to the Awingu appliance and that has at least 1 application running.

Next to this we highly recommend to measure from time to time the overall Awingu appliance resource consumption and when needed add extra resources.

Single node Awingu

In a single node set-up, all processes are running on a single VM (frontend role, backend role and database role). This architecture can support only a limited number of the concurrent users. This has resulted in the following deployment recommendations:

	Concurrent Light Users	Concurrent Heavy Users
2 vCPU + 4 GB memory	100	50
8 vCPU + 8 GB memory	500	100

Note that 4 GiB of RAM is a hard minimum!

Multi node Awingu

Once one Awingu appliance has been installed, you can add other appliances to it to have a multi node Awingu environment (see Service Management Settings). Note that you need a load balancer to balance over the nodes with Frontend roles (see SSL offloader, reverse proxy or loadbalancer settings).

Each appliance can have a Frontend role, a Backend role or both:

- The Frontend role takes care of all RDP and file activity. You need at least 1 of these roles and the more concurrent users you have the more appliances with these roles you need to deploy
- The backend role takes care of the auditing. In a multi node deployment there can only be 1 or 3 backend nodes. No other combinations are allowed.

Next to the Frontend & Backend role there is also a database role: when deploying your first Awingu node there is the option to use the build-in database or go for an external database. This database contains the Awingu configuration and not the audit logs as these are stored in the backend roles. Note it is not possible to change from an internal database to an external database once installation has finished.

If High Availability (HA) is required, i.e. service interruption is not allowed (except during upgrades), then you need at least 3 nodes and an external database (cf. Installation). Note that if an appliance goes down and the Application Sessions Failover feature is enabled users on that node will be disconnected for a few seconds and then be reconnected to an other node. When the feature is not enabled, user sessions on the failing node will be lost and users will have to relogin and restart their apps.

We assume in a multi node environment all nodes are 8 vCPU and 8 GB Memory. The sizing below is for normal operations. In case a node goes down then capacity will be reduced to the capacity of the cluster with 1 node less.

	Roles Configuration	Concurrent Light Users	Concurrent Heavy Users
2 nodes (*)	node 1: Front + Back node 2: Front	1.000	200
3 nodes	node 1,2 & 3 : Front + Back	1.500	300
4 nodes	node 1,2 & 3 : Front + Back node 4: Front	2.000	400
5 nodes	node 1,2 & 3 : Front + Back node 4,5 : Front	2.500	500
...		+ 500	+ 100
10 nodes	node 1,2 & 3 : Front + Back node 4-10: Front	5.000	1.000

(*) A 2-node awingu cluster has no HA. If the first node goes down, there will also be impact on the second node as there are no backend roles anymore available at this time.

Although 10 nodes is not a hard limit we recommend not to go above 10 nodes in a single Awingu cluster. If more users are needed we recommend to setup a second cluster and connect it to the same windows backend.

Also due to split brain reasons, it is recommended to distribute the Backend roles over three differently powered racks.

Backup strategy for multi nodes:

It is always a good practice to regularly backup your Awingu environment, especially before upgrades. If your hypervisor allows **consistent** live snapshots, you can use that feature. If consistency is not guaranteed, then you need to snapshot/backup as follows:

- For backend nodes: please **sequentially** do following actions for each node
    1. Shutdown **one** node
    2. Snapshot/backup the node
    3. Start the node
    4. Wait until all services in the Dashboard are green.
- For frontend nodes: you can shutdown and startup them all at once.
- If you have an external database, please use the snapshot feature of the database to create a consistent snapshot.

Deployment

For your convenience, Awingu provides virtual appliances that are custom-build to run on four commonly used hypervisors, i.e. Microsoft Hyper-V, VMware ESXi, Linux KVM, Citrix XenServer and on three major cloud platforms, i.e. Microsoft Azure, Amazon EC2 and Google Compute. To begin installing the Awingu platform, download the virtual appliance for your hypervisor, import and start the appliance and open your browser to further proceed with your installation through the System Settings. For more detailed instructions describing how to install the Awingu platform on your hypervisor, please have a look at the section below for more detailed instructions specific to your hypervisor.

Supported hypervisors and cloud platforms
Microsoft Hyper-V: 2012 R2 and 2016
VMware ESXi: 6.5 - 7.0
KVM
Citrix XenServer: 7.1
Microsoft Azure
Amazon EC2
Google Compute Engine

- Deployment on Microsoft Hyper-V
- Deployment on VMware ESXi with vSphere Client on Windows
- Deployment on VMware ESXi with vSphere Web Client
- Deployment on Linux KVM
- Deployment on Microsoft Azure
- Deployment on Amazon EC2
- Deployment on Google Compute

Deployment on Microsoft Hyper-V

In this guide we will show you how to deploy the Awingu appliance on Microsoft Hyper-v hypervisor using Microsoft Hyper-V manager

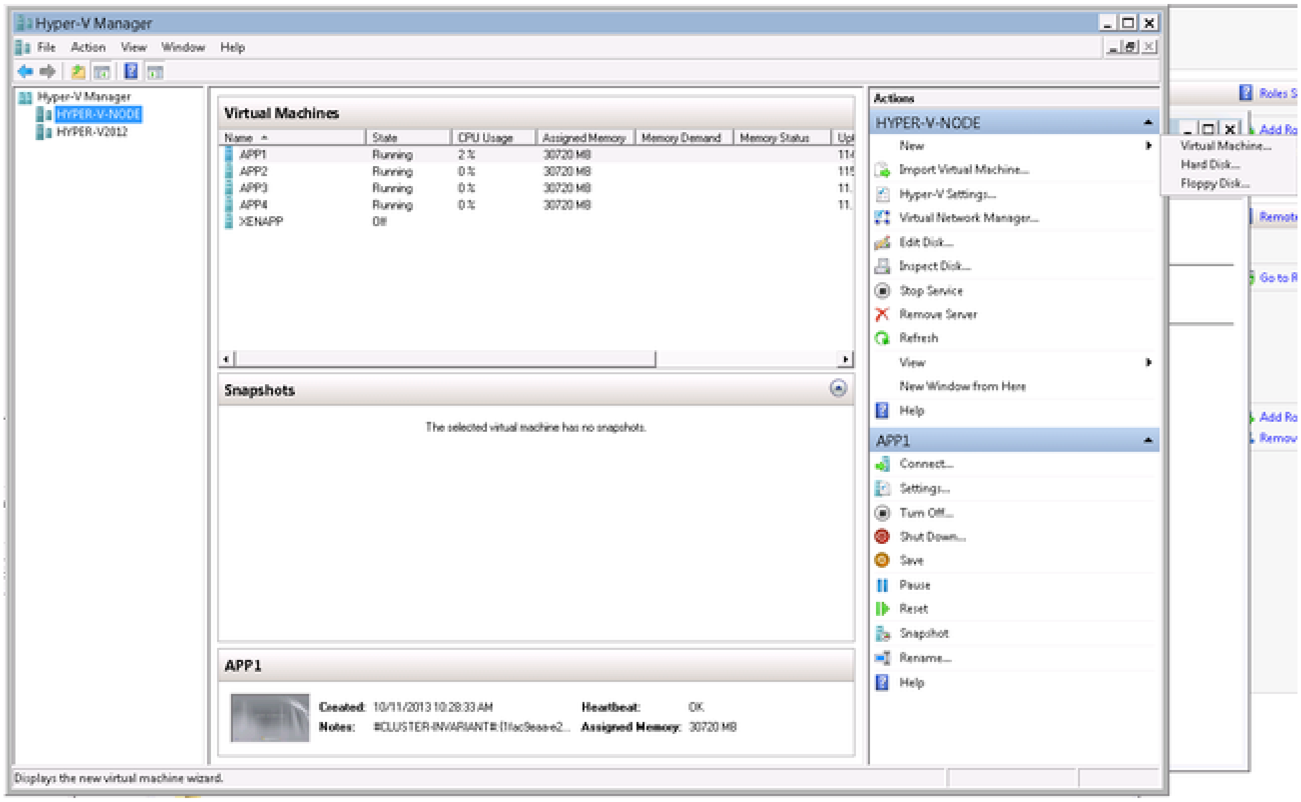
- Step 1 - Download and extract the Awingu appliance
- Step 2 - Create a VM with the VHD image in Hyper-V manager
- Step 3 - Start up the Awingu virtual machine

Step 1 - Download and extract the Awingu appliance

Download the Awingu appliance from the Awingu repository server at https://repo-pub.awingu.com/appliances/latest/vhd/ and extract the ZIP file to obtain the VHD.

Step 2 - Create a VM with the VHD image in Hyper-V manager

1. Import the VHD image in Hyper-V manager by choosing the option "New Virtual Machine".



Virtual Machines

Name	State	CPU Usage	Assigned Memory	Memory Demand	Memory Status	Up
APP1	Running	2 %	30720 MB			114
APP2	Running	0 %	30720 MB			115
APP3	Running	0 %	30720 MB			11.
APP4	Running	0 %	30720 MB			11.
XENAPP	Off					

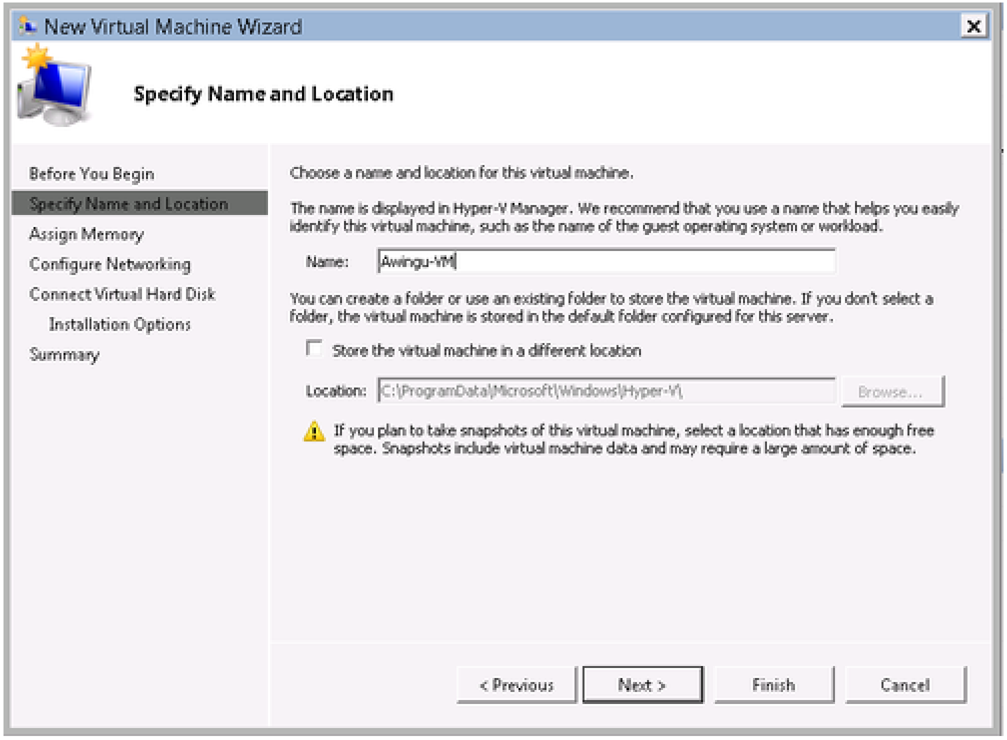
The selected virtual machine has no snapshots.

APP1

Created: 10/11/2013 10:28:33 AM
Notes: #CLUSTER-INVARIANT#:{11ac9eaa-e2...
Heartbeat: OK
Assigned Memory: 30720 MB

Displays the new virtual machine wizard.

2. Specify a name for the Awingu virtual machine



Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: Awingu-VM

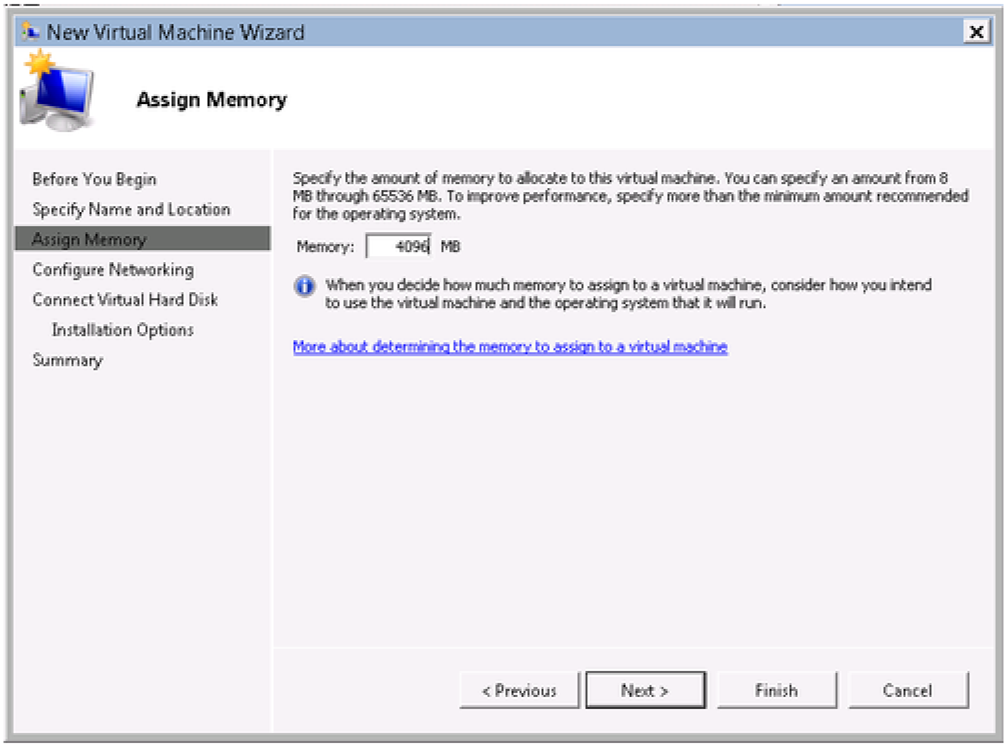
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

□ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.

3. Assign memory to the Awingu virtual machine:
4. Specify RAM and CPU settings for your VM. See Sizing & Scaling Requirements to determine the hardware requirements.



Assign Memory

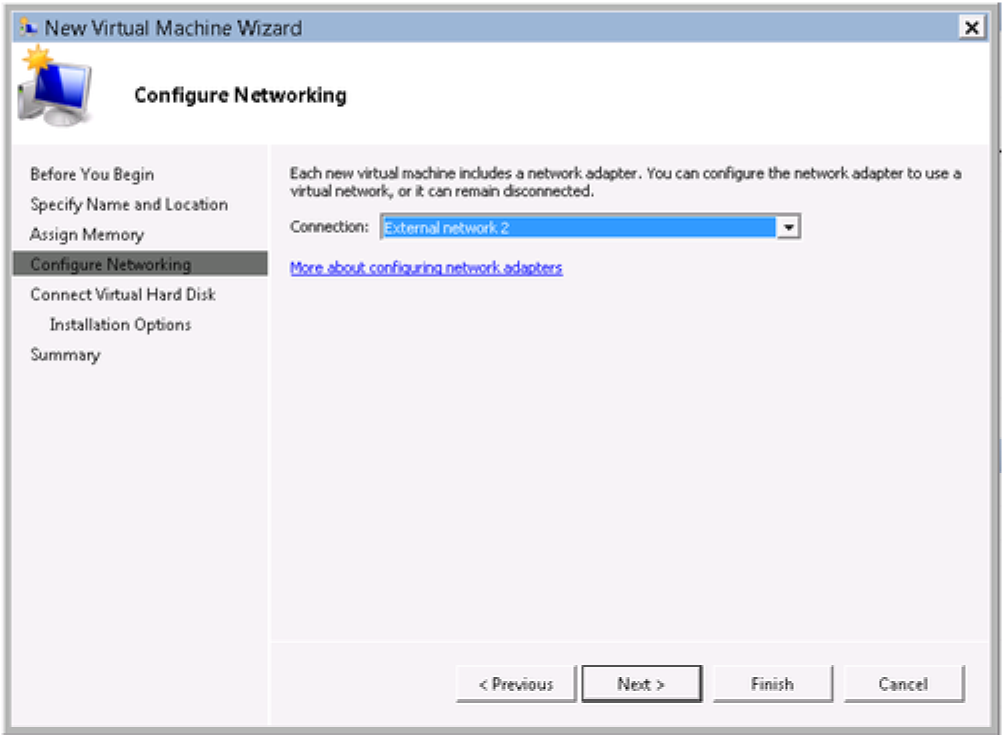
Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 65536 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Memory: 4096 MB

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

More about determining the memory to assign to a virtual machine

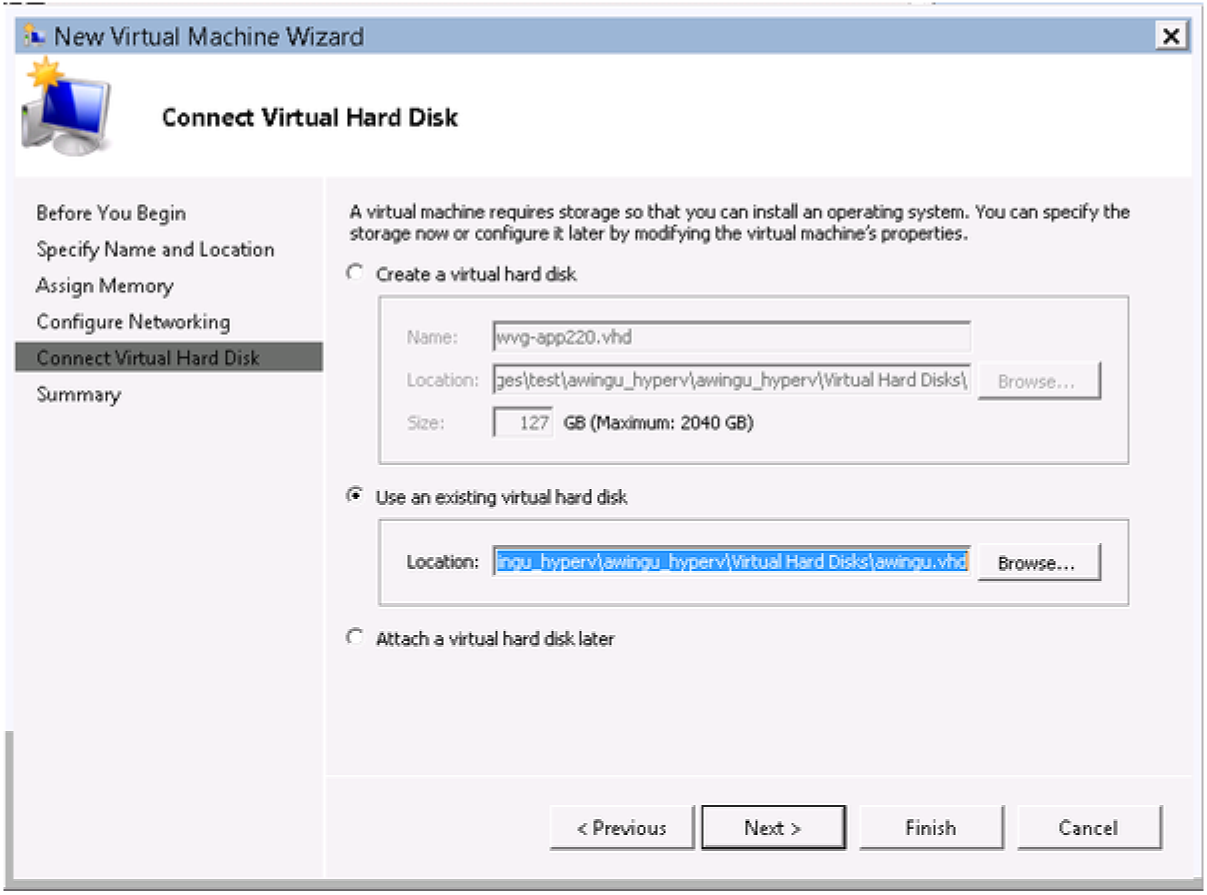
5. Configure networking for your Awingu virtual machine



Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual network, or it can remain disconnected.

Connection: External network 2

6. Connect to a virtual hard disk by selecting the option **"Use an existing virtual hard disk"**. Select the unzipped VHD file.



A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Name: wvg-app220.vhd

Location: ges\test\awingu_hyperv\awingu_hyperv\Virtual Hard Disks\

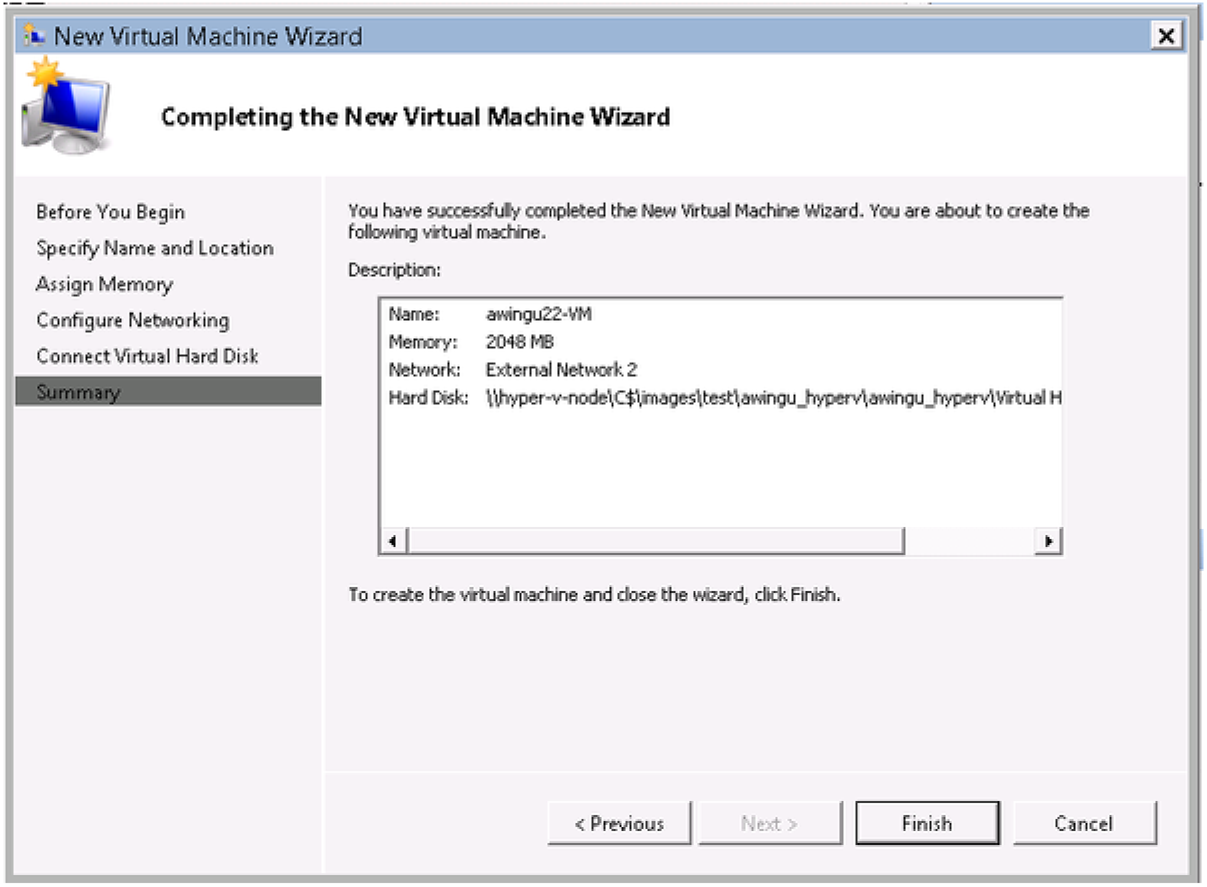
Size: 127 GB (Maximum: 2040 GB)

● Use an existing virtual hard disk

Location: ingu_hyperv\awingu_hyperv\Virtual Hard Disks\awingu.vhd

○ Attach a virtual hard disk later

7. Review your virtual machine settings



Completing the New Virtual Machine Wizard

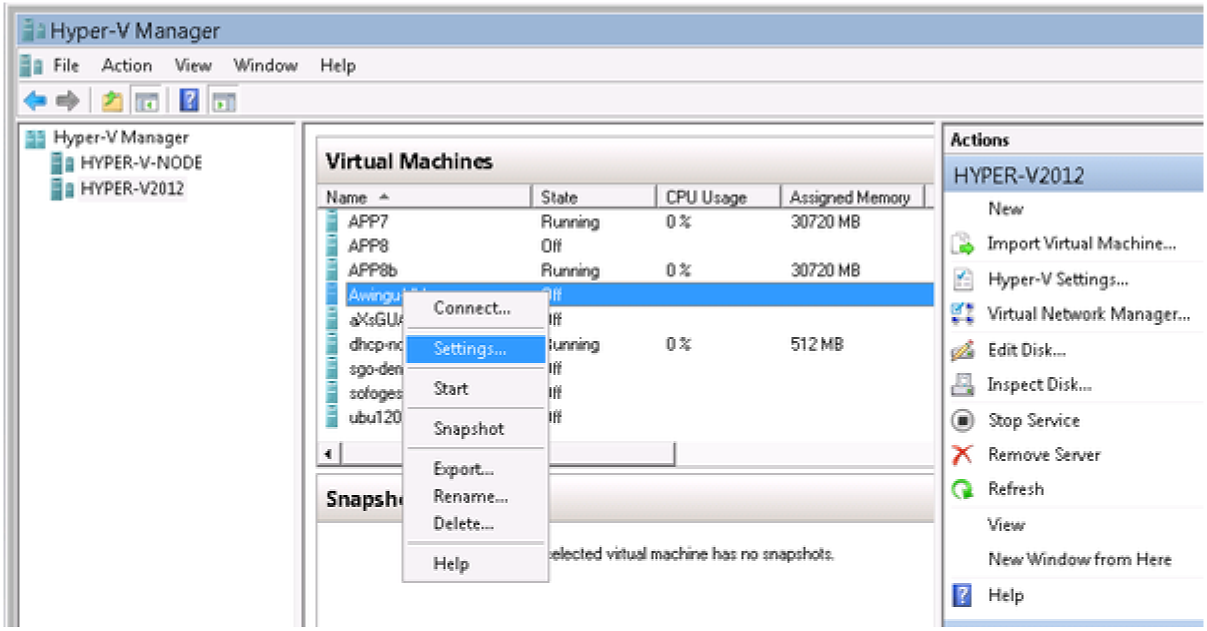
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name:	awingu22-VM
Memory:	2048 MB
Network:	External Network 2
Hard Disk:	\\hyper-v-node\C$\images\test\awingu_hyperv\awingu_hyperv\Virtual H

To create the virtual machine and close the wizard, click Finish.

8. Right click on the Awingu Virtual machine and click "settings..."



Virtual Machines

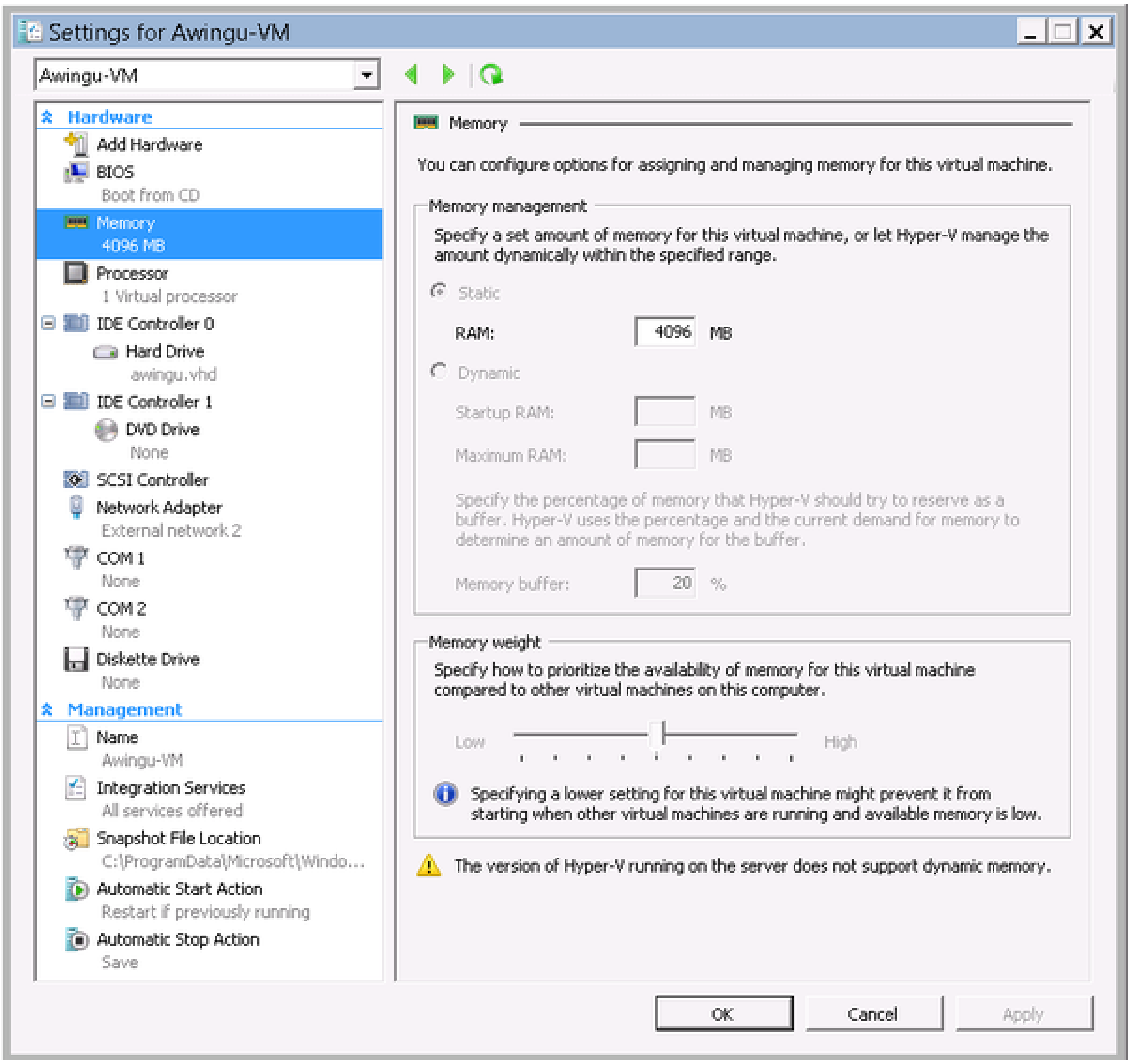
Name	State	CPU Usage	Assigned Memory
APP7	Running	0 %	30720 MB
APP8	Off		
APP8b	Running	0 %	30720 MB
Awingu	ff		
aXsGUI	ff		
dhcp-nc	unning	0 %	512 MB
sgo-den	ff		
sofoges	ff		
ubu120	ff		

Snapsh

elected virtual machine has no snapshots.

9. Please edit the settings of the Awingu-VM to specify the memory and CPU settings:

> In memory management, make sure you select **"Static"**. Dynamic memory allocation is not supported in Hyper-V manager for debian-based Linux Systems, so selecting "Dynamic" will result in errors on your VM.



Settings for Awingu-VM

Awingu-VM

Hardware
- Add Hardware
- BIOS
  Boot from CD
- Memory
  4096 MB
- Processor
  1 Virtual processor
- IDE Controller 0
  - Hard Drive
    awingu.vhd
- IDE Controller 1
  - DVD Drive
    None
- SCSI Controller
- Network Adapter
  External network 2
- COM 1
  None
- COM 2
  None
- Diskette Drive
  None

Management
- Name
  Awingu-VM
- Integration Services
  All services offered
- Snapshot File Location
  C:\ProgramData\Microsoft\Windo...
- Automatic Start Action
  Restart if previously running
- Automatic Stop Action
  Save

Memory

You can configure options for assigning and managing memory for this virtual machine.

Memory management

Specify a set amount of memory for this virtual machine, or let Hyper-V manage the amount dynamically within the specified range.

● Static

RAM: 4096 MB

○ Dynamic

Startup RAM: MB

Maximum RAM: MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer: 20 %

Memory weight

Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

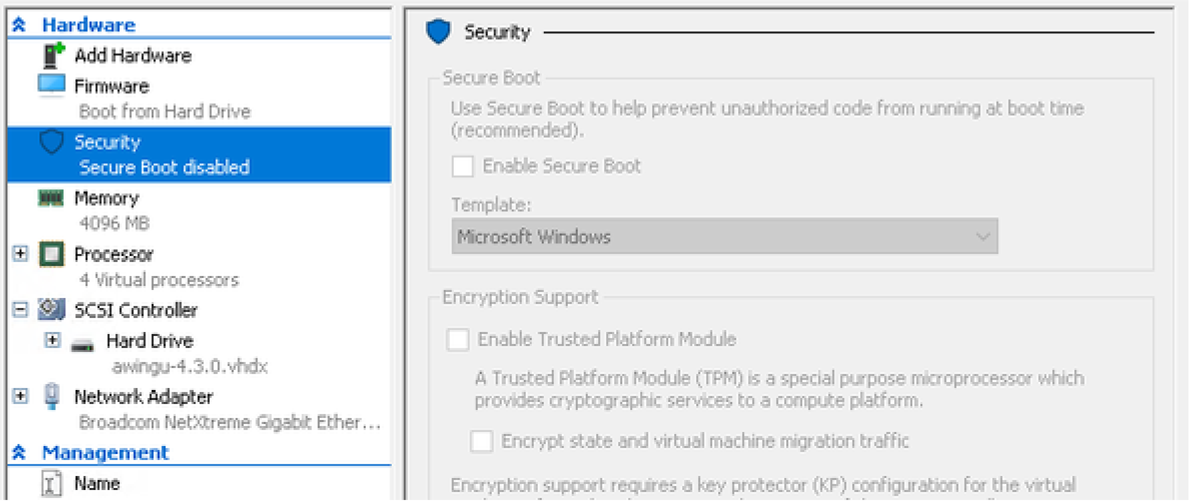
Low — High

Specifying a lower setting for this virtual machine might prevent it from starting when other virtual machines are running and available memory is low.

⚠ The version of Hyper-V running on the server does not support dynamic memory.

OK Cancel Apply

10. Disable Secure boot in the Security section of the settings when using Generation 2 VMs



Hardware
- Add Hardware
- Firmware
  Boot from Hard Drive
- Security
  Secure Boot disabled
- Memory
  4096 MB
- Processor
  4 Virtual processors
- SCSI Controller
  - Hard Drive
    awingu-4.3.0.vhdx
- Network Adapter
  Broadcom NetXtreme Gigabit Ether...

Management
- Name

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

□ Enable Secure Boot

Template:

Microsoft Windows

Encryption Support

□ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

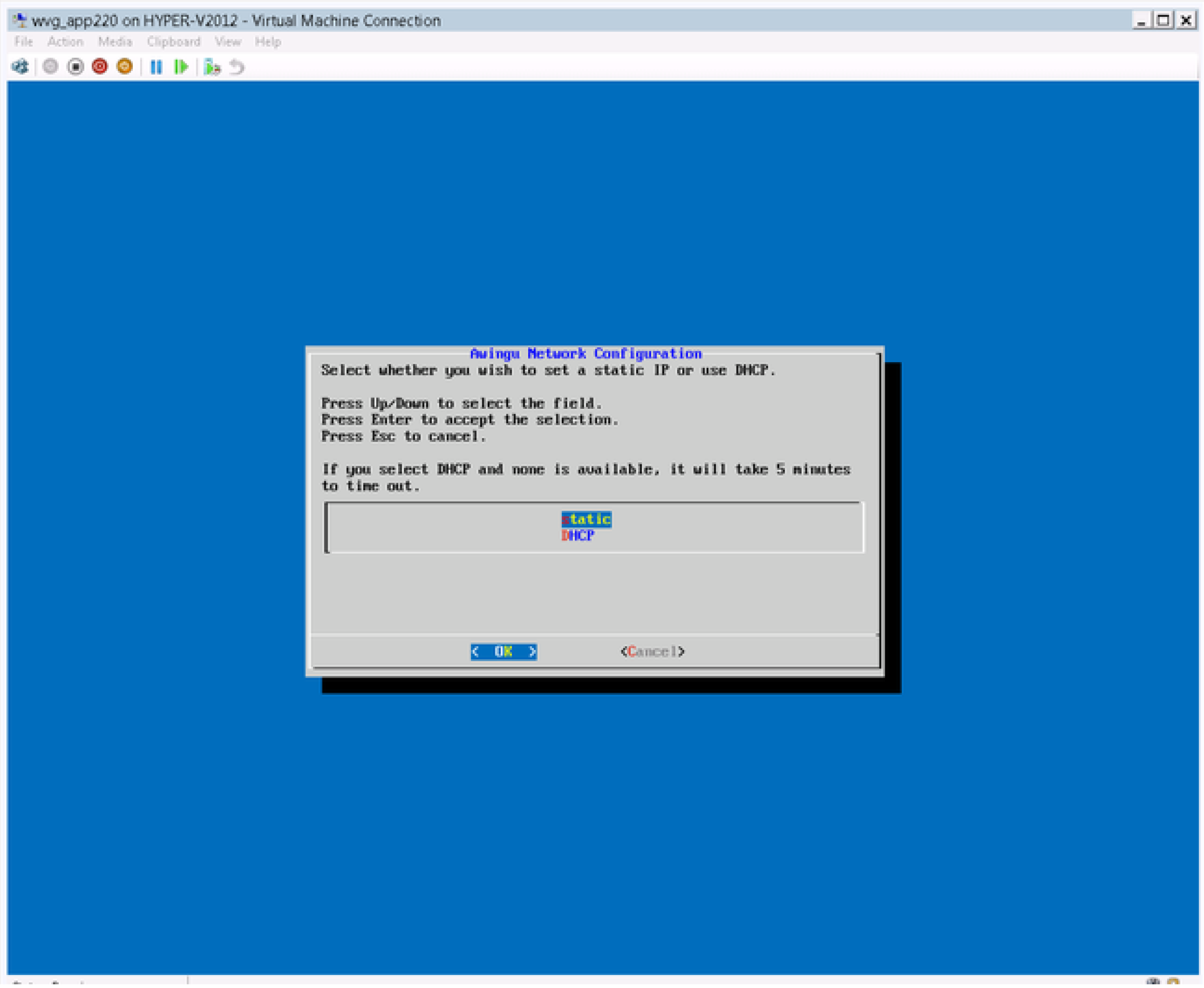
□ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual

Step 3 - Start up the Awingu virtual machine

1. Open a console to connect to the virtual machine.

2. Configure the virtual machine network settings. You can choose to use either a static IP or a dynamic IP assigned by DHCP.



wvg_app220 on HYPER-V2012 - Virtual Machine Connection
File Action Media Clipboard View Help

```
Awingu Network Configuration
Select whether you wish to set a static IP or use DHCP.

Press Up/Down to select the field.
Press Enter to accept the selection.
Press Esc to cancel.

If you select DHCP and none is available, it will take 5 minutes
to time out.

                    Static
                    DHCP

            <  OK  >            <Cancel>
```

3. After you have configured your network settings, you are now ready to proceed with the installation through a graphical installer interface. If you need to change your network settings in the future, you can update these here again (not supported for multi node configuration).
   In order to connect to the graphical installer interface, open a web browser and browse to the IP of the Awingu virtual machine on port 8080. More information about how to proceed with the install can be found here.

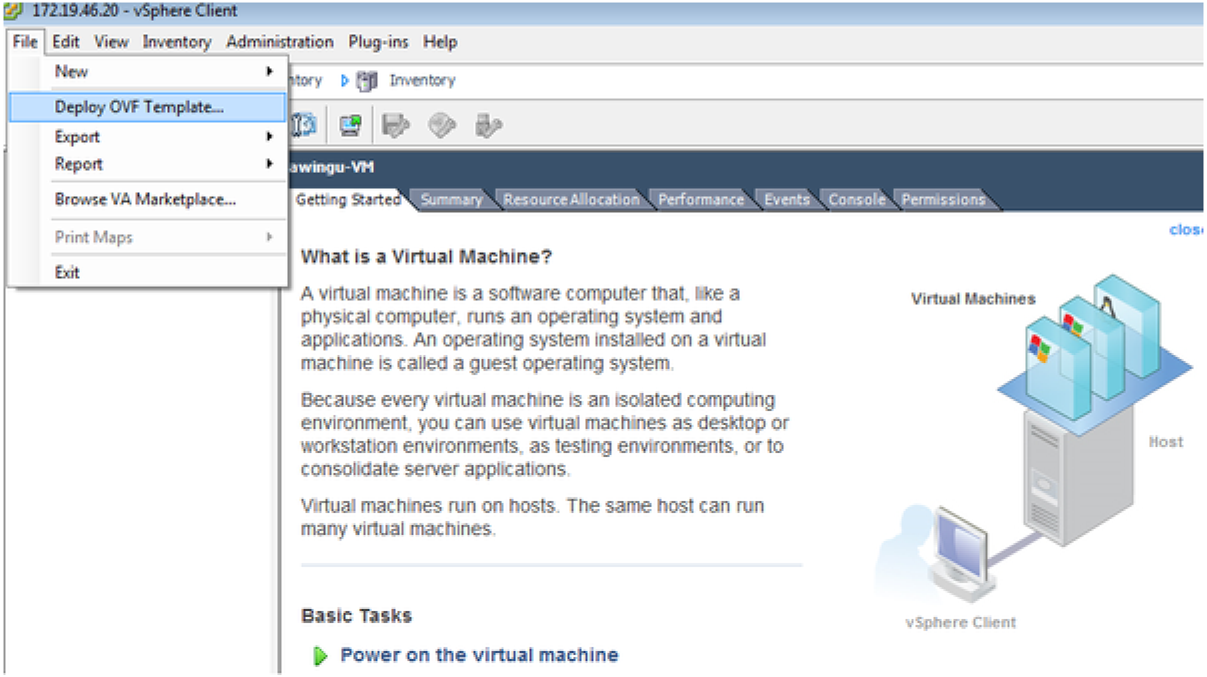
Deployment on VMware ESXi with vSphere Client on Windows

In this guide we will show you how to install and deploy the Awingu appliance on VMware ESXi hypervisor.

- Step 1 - Import the appliance in VMware vSphere Client
- Step 2 - Configure your Awingu virtual machine settings
- Step 3 - Start up your Awingu virtual machine

Step 1 - Import the appliance in VMware vSphere Client

1. Connect to your vShpere ESXi hypervisor using vSphere Client
2. Open the OVF deployment menu



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

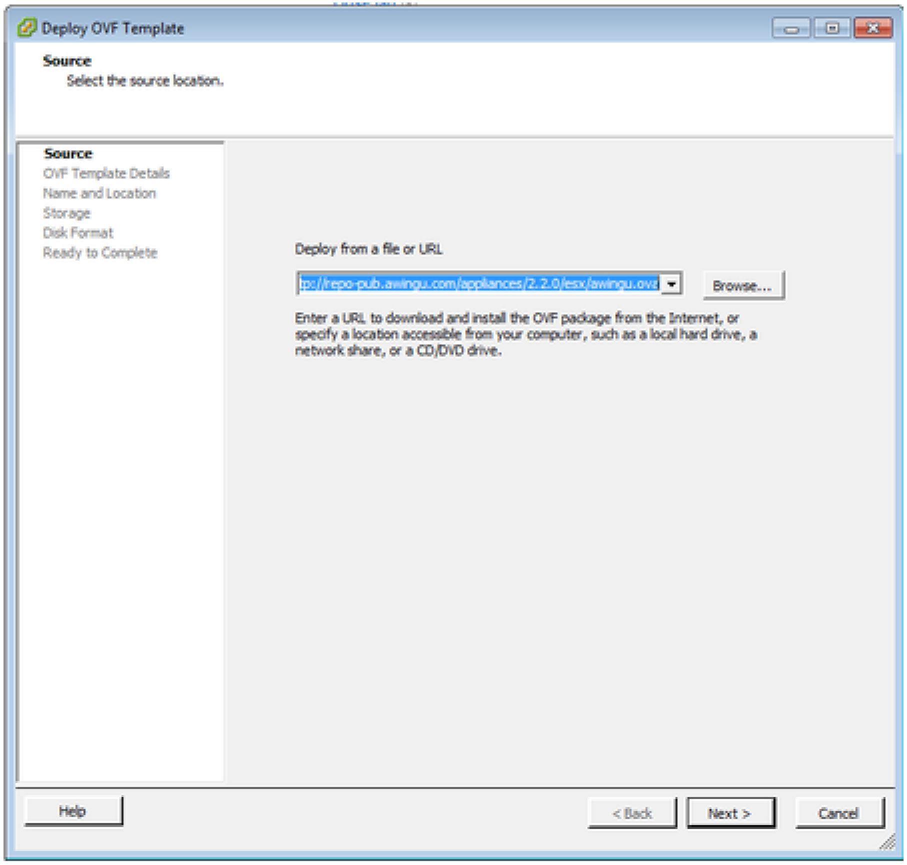
Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

Power on the virtual machine

3. Import the Awingu OVF template from the Awingu repo server
    a. Go to https://repo-pub.awingu.com/appliances/latest/ and browse to the ESX directory.

b. Select the OVA file you want to download and copy-paste this URL in your VMware client import menu:
E.g.: https://repo-pub.awingu.com/appliances/latest/esx/awingu-4-0-1.ova



Source
Select the source location.

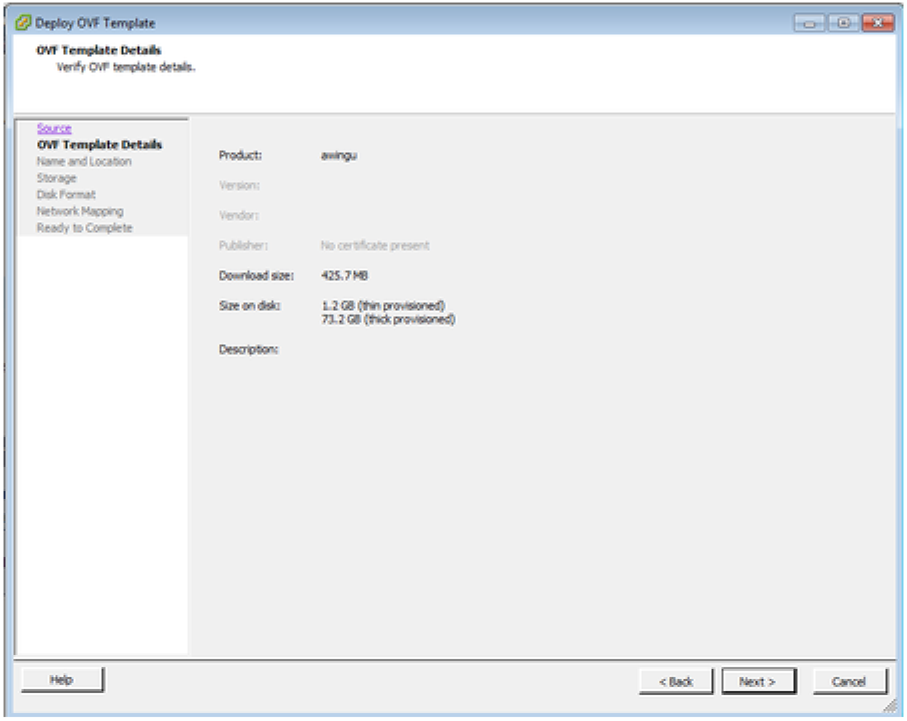
Deploy from a file or URL

tp://repo-pub.awingu.com/appliances/2.2.0/esx/awingu.ova

Enter a URL to download and install the OVF package from the Internet, or specify a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

c. Alternatively, you can download the OVA file and use it via the Browse... button.

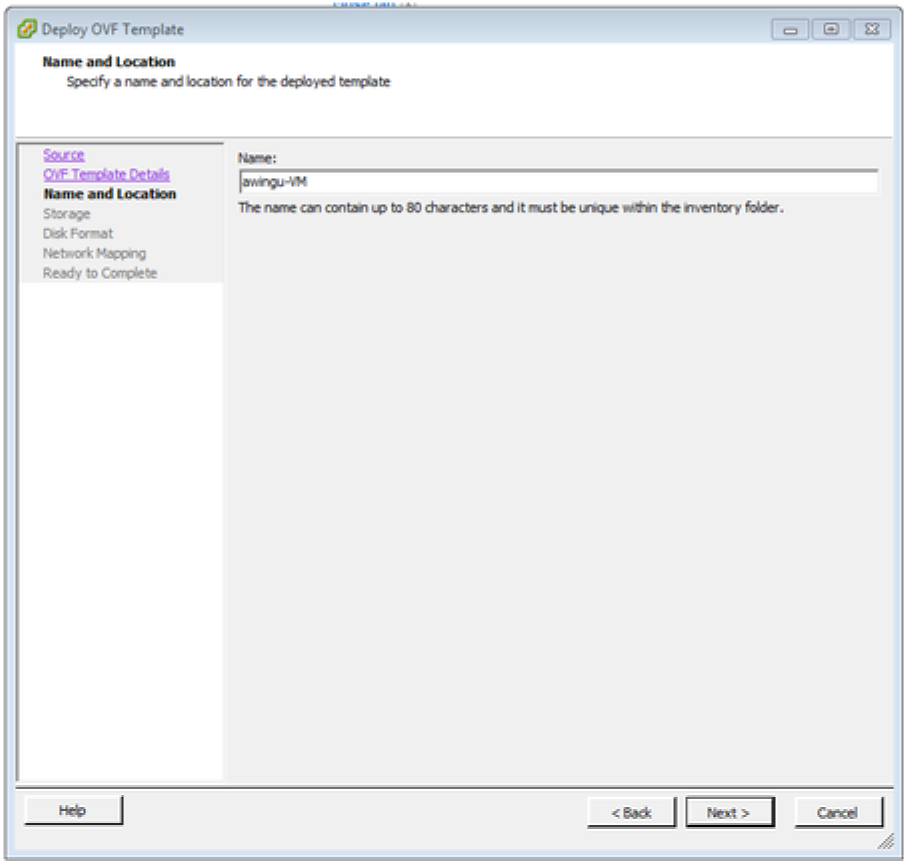
4. Verify the template details



OVF Template Details
Verify OVF template details.

Product: awingu
Version:
Vendor:
Publisher: No certificate present
Download size: 425.7 MB
Size on disk: 1.2 GB (thin provisioned)
73.2 GB (thick provisioned)
Description:

5. Enter the name for your Awingu virtual machine



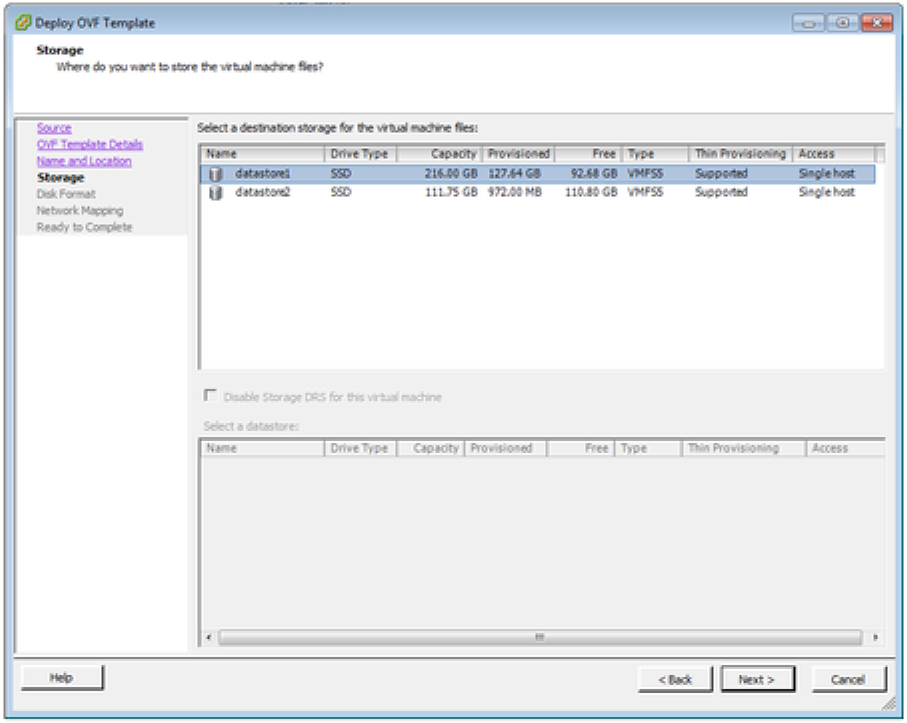
Name and Location

Specify a name and location for the deployed template

Name:
awingu-VM

The name can contain up to 80 characters and it must be unique within the inventory folder.

6. Select the data storage where you want to store your virtual machine



Storage

Where do you want to store the virtual machine files?

Select a destination storage for the virtual machine files:

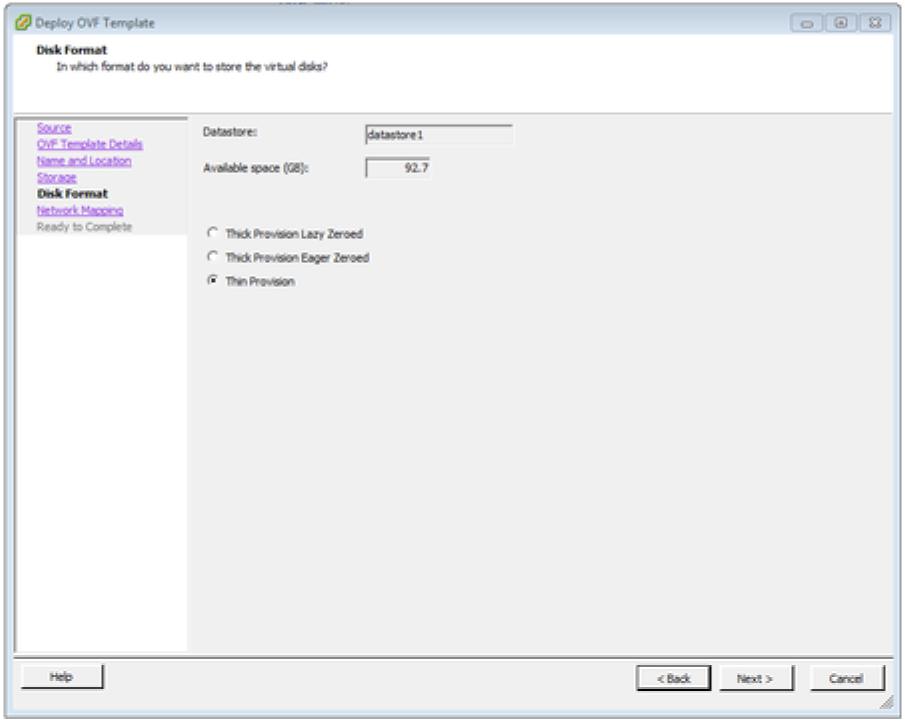
Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning	Access
datastore1	SSD	216.00 GB	127.64 GB	92.68 GB	VMFS5	Supported	Single host
datastore2	SSD	111.75 GB	972.00 MB	110.80 GB	VMFS5	Supported	Single host

☐ Disable Storage DRS for this virtual machine

Select a datastore:

Name	Drive Type	Capacity	Provisioned	Free	Type	Thin Provisioning	Access

7. Select "Thin provision"



Disk Format

In which format do you want to store the virtual disks?

Datastore: datastore1

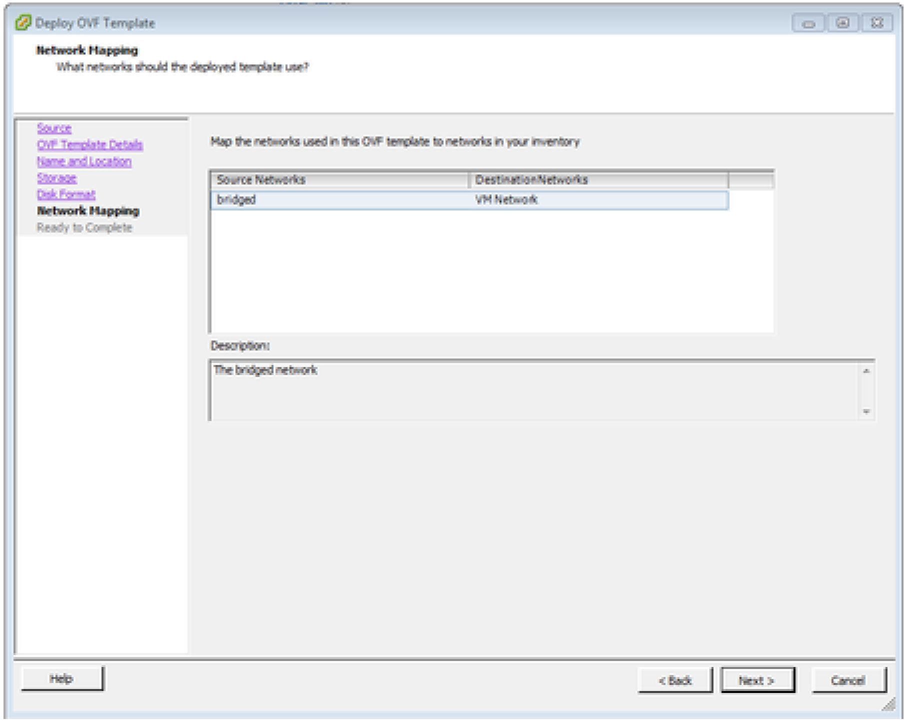
Available space (GB): 92.7

○ Thick Provision Lazy Zeroed

○ Thick Provision Eager Zeroed

● Thin Provision

8. Set network mode for your virtual machine to "bridged"



Network Mapping

What networks should the deployed template use?

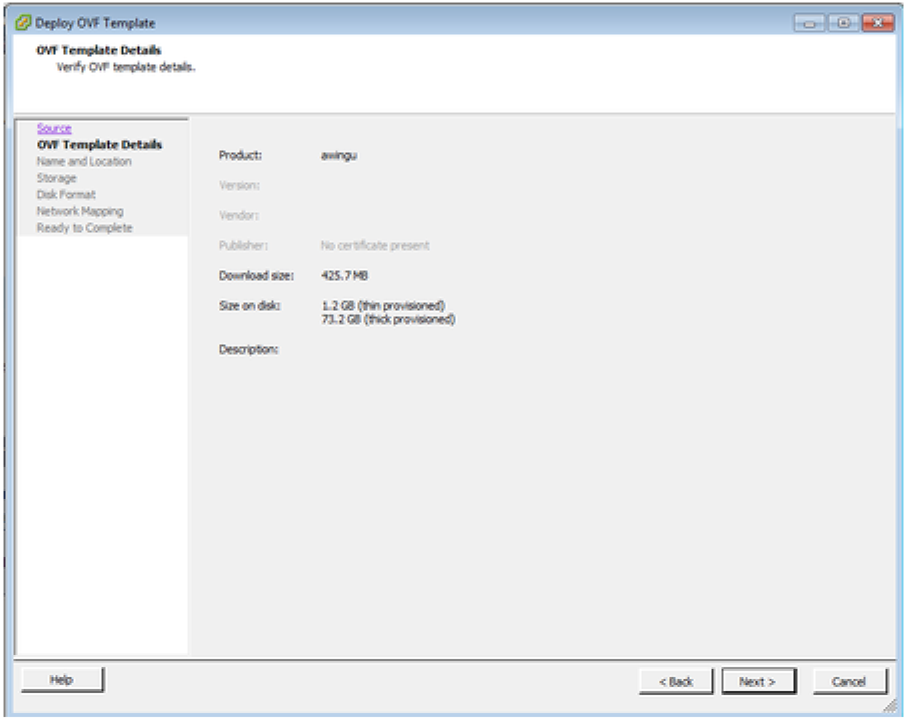
Map the networks used in this OVF template to networks in your inventory

Source Networks	DestinationNetworks
bridged	VM Network

Description:

The bridged network

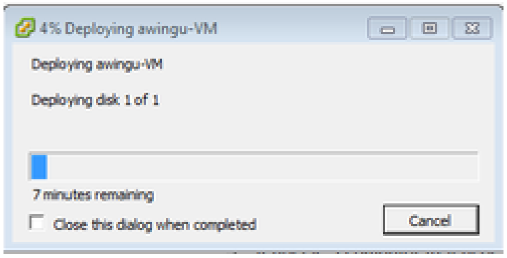
9. Review your configuration and go back to change details if needed



OVF Template Details
Verify OVF template details.

Product: awingu
Version:
Vendor:
Publisher: No certificate present
Download size: 425.7 MB
Size on disk: 1.2 GB (thin provisioned)
73.2 GB (thick provisioned)
Description:

10. Click finish to start download and deploy the Awingu appliance. This step may take several minutes. Do **not start** the machine automatically after deployment.



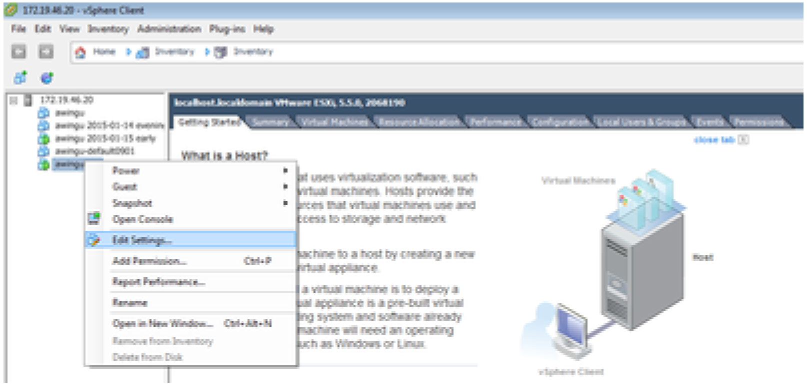
Deploying awingu-VM

Deploying disk 1 of 1

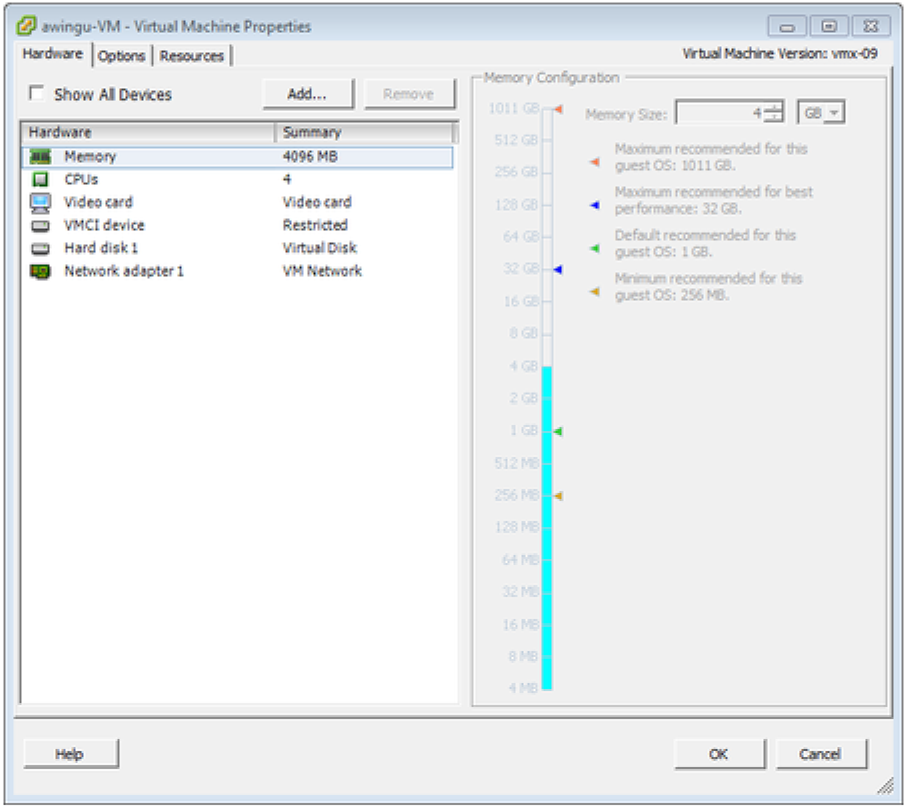
7 minutes remaining

Step 2 - Configure your Awingu virtual machine settings

1. Right-click on the Awingu-VM to change the settings for RAM and CPUs:



2. You can now allocate memory and CPU sources to the Awingu Virtual Machine



awingu-VM - Virtual Machine Properties

Virtual Machine Version: vmx-09

□ Show All Devices

Hardware	Summary
Memory	4096 MB
CPUs	4
Video card	Video card
VMCI device	Restricted
Hard disk 1	Virtual Disk
Network adapter 1	VM Network

Memory Configuration

Memory Size: 4 GB

Maximum recommended for this guest OS: 1011 GB.

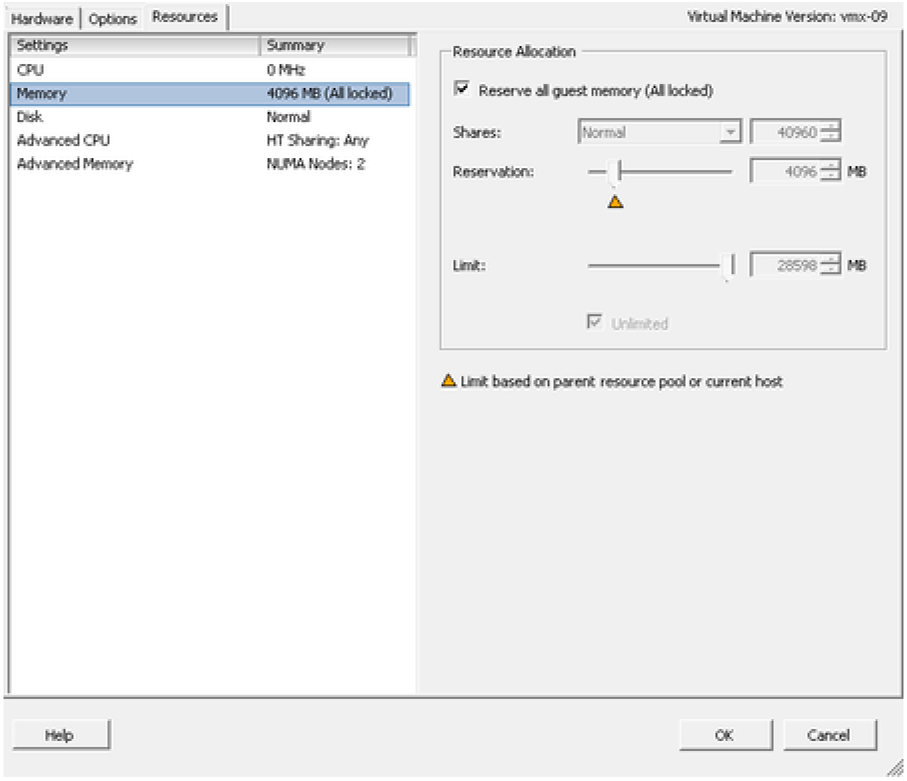
Maximum recommended for best performance: 32 GB.

Default recommended for this guest OS: 1 GB.

Minimum recommended for this guest OS: 256 MB.

See Sizing & Scaling Requirements to determine the hardware requirements.

3. When the host's memory is almost full, ESXi will start doing memory ballooning on the Virtual Machines. Ballooning is not recommended for the Awingu. To avoid this, you can reserve all memory:



Virtual Machine Version: vmx-09

Settings	Summary
CPU	0 MHz
Memory	4096 MB (All locked)
Disk	Normal
Advanced CPU	HT Sharing: Any
Advanced Memory	NUMA Nodes: 2

Resource Allocation

☑ Reserve all guest memory (All locked)

Shares: Normal 40960

Reservation: 4096 MB

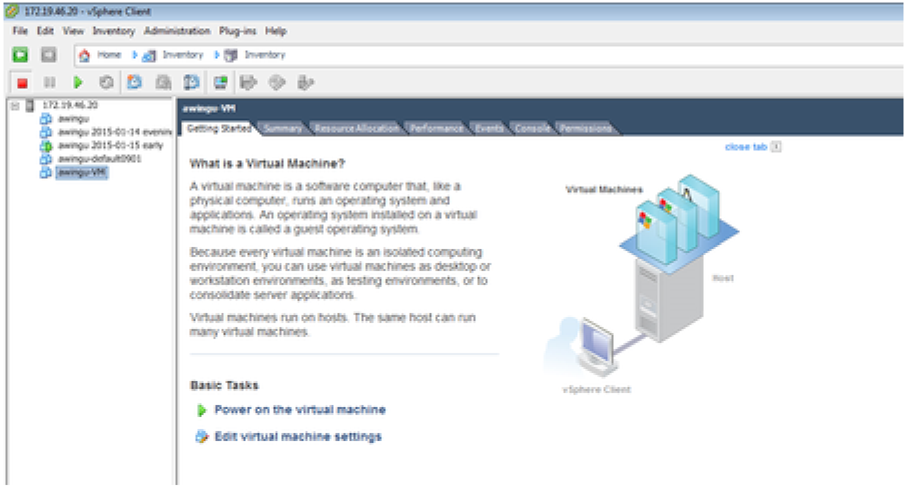
Limit: 28598 MB

☑ Unlimited

⚠ Limit based on parent resource pool or current host

Step 3 - Start up your Awingu virtual machine

1. Start up the virtual machine in your VMware inventory view and open the console of the Awingu virtual machine



What is a Virtual Machine?

A virtual machine is a software computer that, like a physical computer, runs an operating system and applications. An operating system installed on a virtual machine is called a guest operating system.

Because every virtual machine is an isolated computing environment, you can use virtual machines as desktop or workstation environments, as testing environments, or to consolidate server applications.

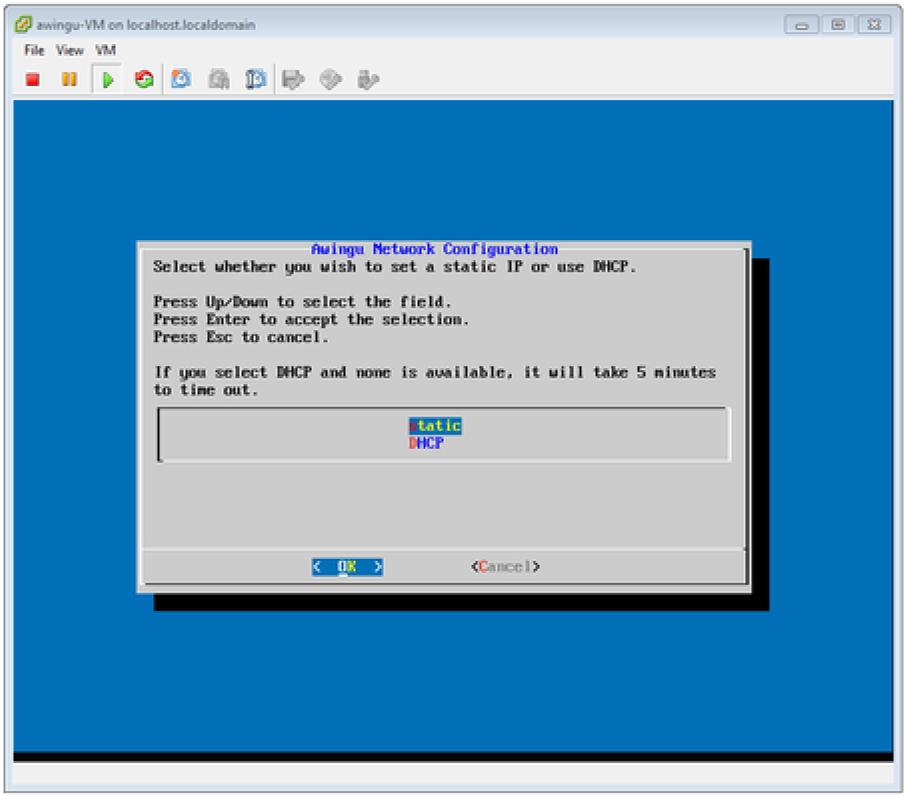
Virtual machines run on hosts. The same host can run many virtual machines.

Basic Tasks

Power on the virtual machine

Edit virtual machine settings

2. After booting the machine you should be presented a network configuration menu where you can choose to use a static IP address or to use a dynamic IP address assigned through DHCP:



```
Awingu Network Configuration
Select whether you wish to set a static IP or use DHCP.

Press Up/Down to select the field.
Press Enter to accept the selection.
Press Esc to cancel.

If you select DHCP and none is available, it will take 5 minutes
to time out.

                        Static
                        DHCP

              <  OK  >           <Cancel>
```

3. After you have configured your network settings you can now go to the graphical installation interface. If you need to change your network settings in the future, you can update these here again (not supported for multi node configuration).
More detailed instructions how to proceed with the graphical installer interface can be found in the next section.

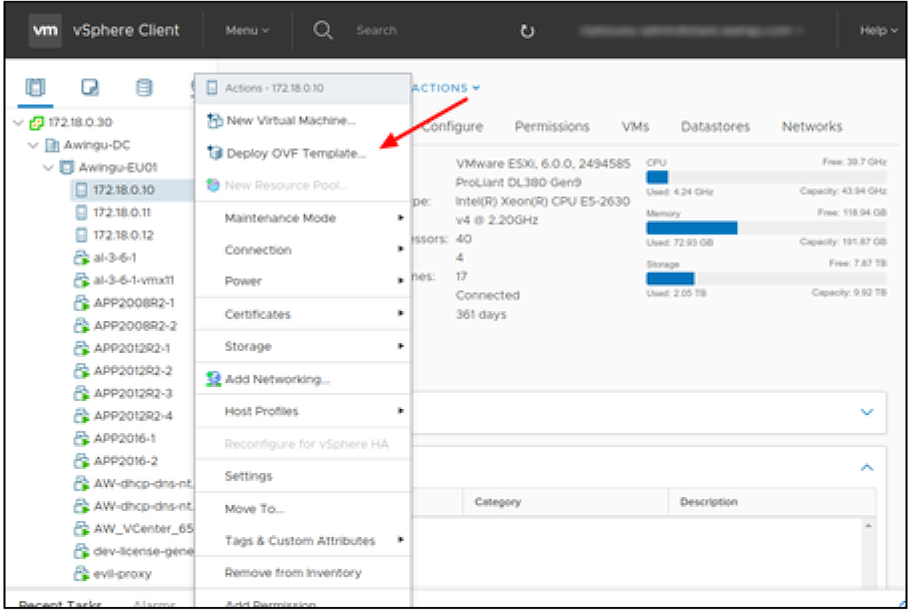
Deployment on VMware ESXi with vSphere Web Client

In this guide we will show you how to install and deploy the Awingu appliance on VMware vCenter.

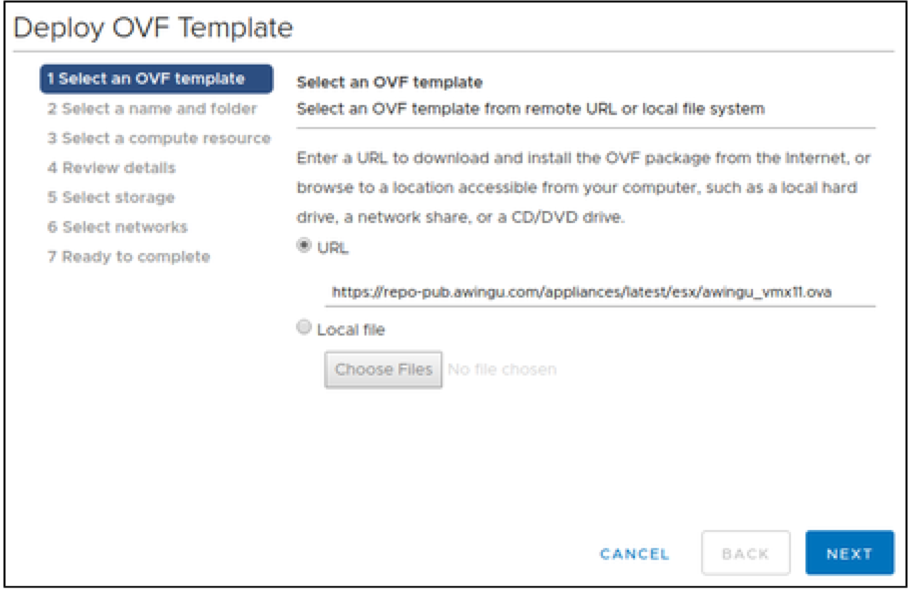
- Step 1 - Import the appliance in VMware vSphere Client
- Step 2 - Configure your Awingu virtual machine settings
- Step 3 - Start up your Awingu virtual machine

Step 1 - Import the appliance in VMware vSphere Client

1. Connect to vCenter using vSphere Client (HTML5 or Flash)
2. In the left column, navigate to your hypervisor, right-click and select *Deploy OVF Template...*



3. Import the Awingu OVF template from the Awingu repo server
   a. Go to https://repo-pub.awingu.com/appliances/latest/ and browse to the ESX directory.
   b. Select the OVA file and copy-paste this URL the *Deploy OVF Template* wizard:
   E.g.: https://repo-pub.awingu.com/appliances/latest/esx/awingu-4-0-1.ova



Deploy OVF Template

1 Select an OVF template
2 Select a name and folder
3 Select a compute resource
4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Select an OVF template

Select an OVF template from remote URL or local file system

Enter a URL to download and install the OVF package from the Internet, or browse to a location accessible from your computer, such as a local hard drive, a network share, or a CD/DVD drive.

● URL

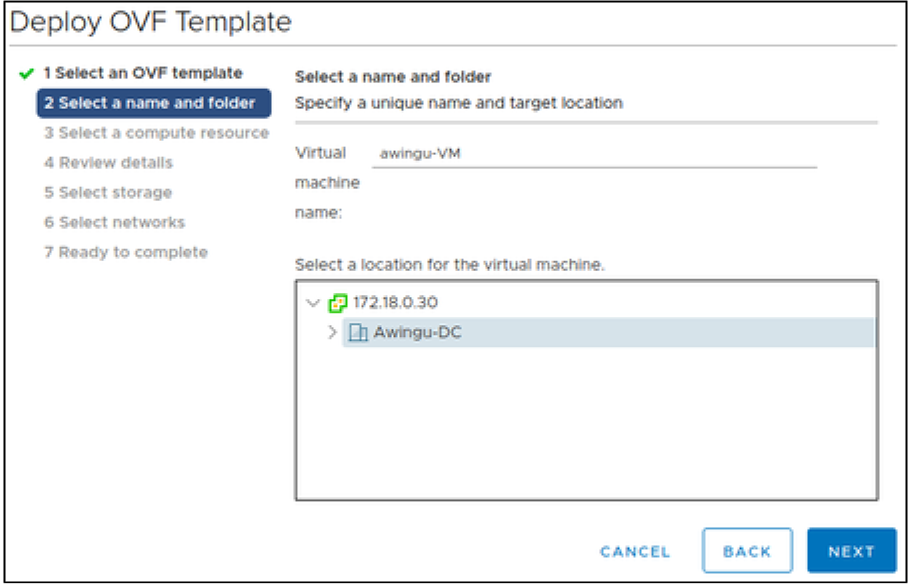
https://repo-pub.awingu.com/appliances/latest/esx/awingu_vmx11.ova

○ Local file

Choose Files No file chosen

   c. Alternatively, you can download the OVA file upload it via the *Local file* option.

4. Enter the name for your Awingu virtual machine and select the location.



Select a name and folder

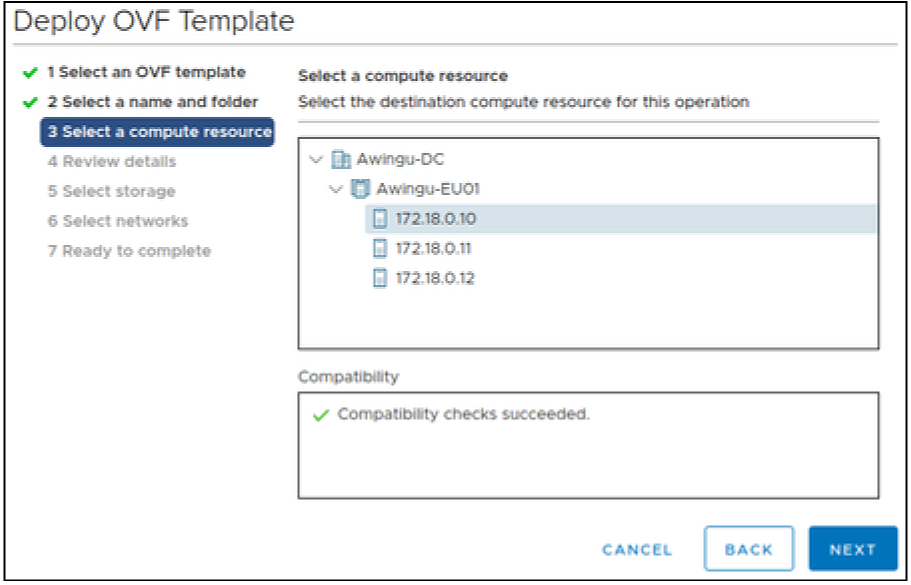
Specify a unique name and target location

Virtual machine name: awingu-VM

Select a location for the virtual machine.

```
172.18.0.30
  > Awingu-DC
```

5. Select the hypervisor to deploy on.



Select a compute resource

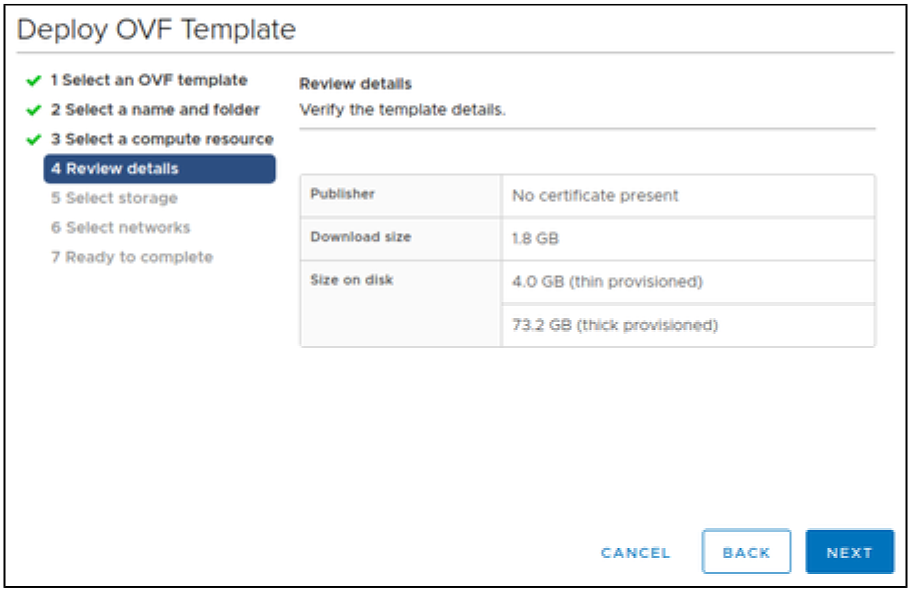
Select the destination compute resource for this operation

```
Awingu-DC
  Awingu-EU01
    172.18.0.10
    172.18.0.11
    172.18.0.12
```

Compatibility

✓ Compatibility checks succeeded.

6. Review the details.

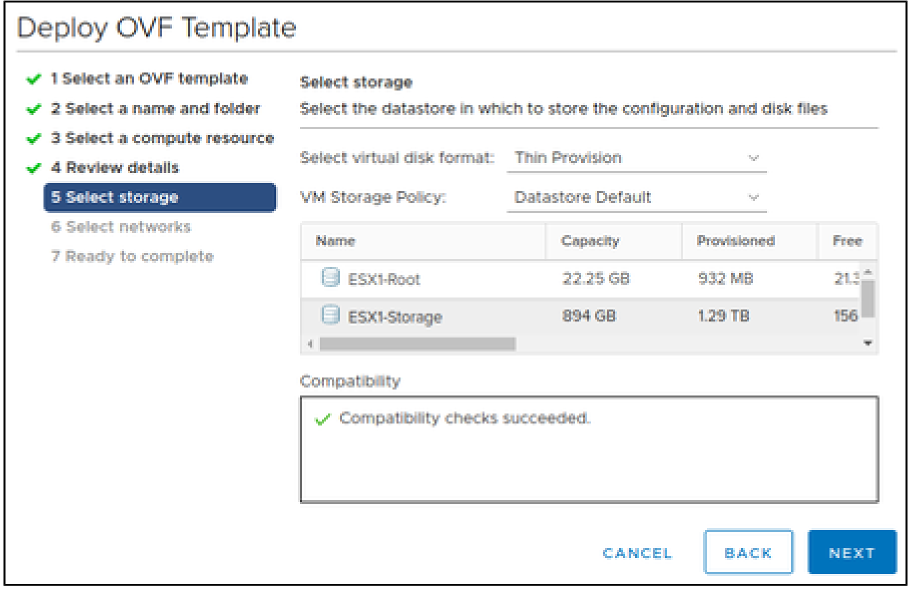


Review details

Verify the template details.

Publisher	No certificate present
Download size	1.8 GB
Size on disk	4.0 GB (thin provisioned)
	73.2 GB (thick provisioned)

7. Select the storage options and location. Note that Thin Provisioning works fine.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
5 Select storage
6 Select networks
7 Ready to complete

Select storage

Select the datastore in which to store the configuration and disk files

Select virtual disk format: Thin Provision

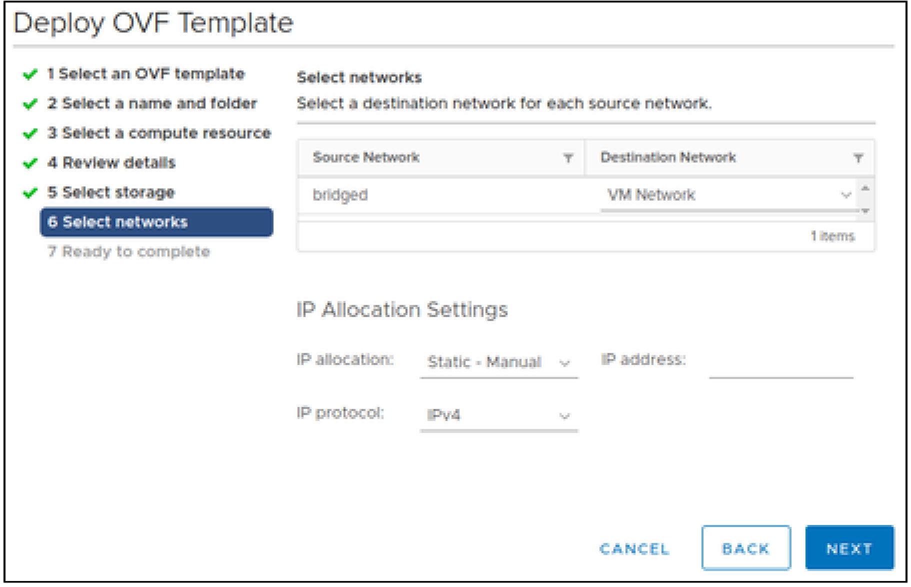
VM Storage Policy: Datastore Default

Name	Capacity	Provisioned	Free
ESX1-Root	22.25 GB	932 MB	21.3
ESX1-Storage	894 GB	1.29 TB	156

Compatibility

✓ Compatibility checks succeeded.

8. Set network mode for your virtual machine to "bridged". You don't need to provide an IP address.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 Select storage
6 Select networks
7 Ready to complete

Select networks

Select a destination network for each source network.

Source Network	Destination Network
bridged	VM Network

1 items

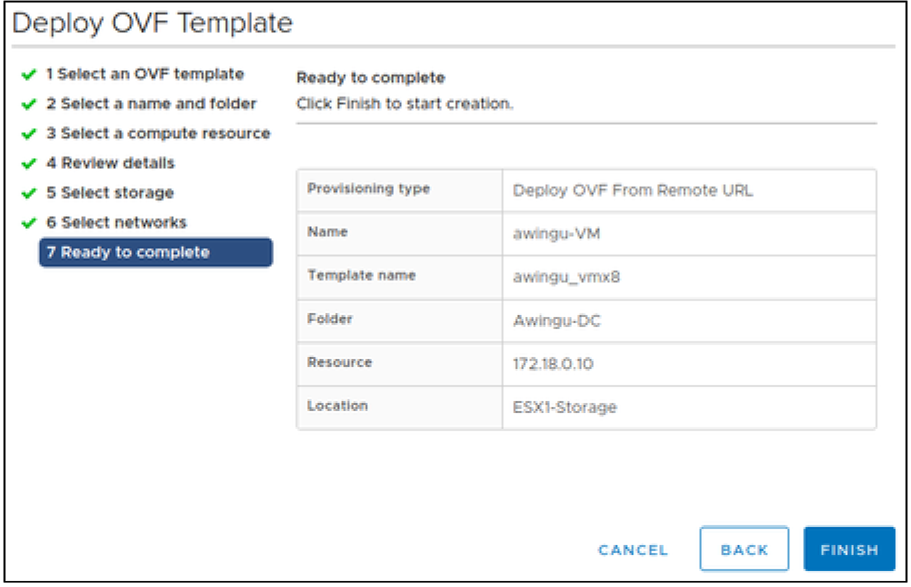
IP Allocation Settings

IP allocation: Static - Manual

IP address:

IP protocol: IPv4

9. Review your configuration and go back to change details if needed.



Deploy OVF Template

✓ 1 Select an OVF template
✓ 2 Select a name and folder
✓ 3 Select a compute resource
✓ 4 Review details
✓ 5 Select storage
✓ 6 Select networks
7 Ready to complete

Ready to complete

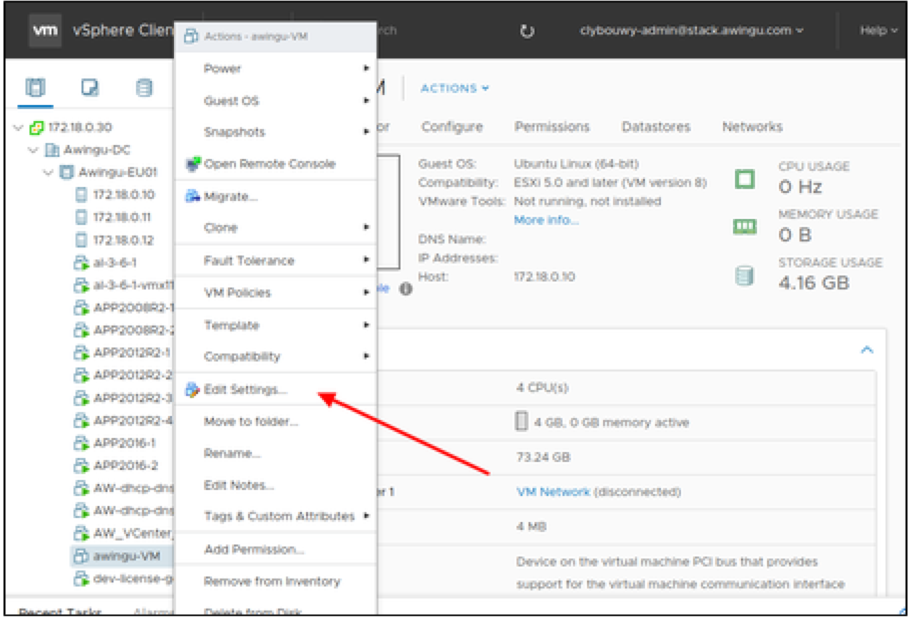
Click Finish to start creation.

Provisioning type	Deploy OVF From Remote URL
Name	awingu-VM
Template name	awingu_vmx8
Folder	Awingu-DC
Resource	172.18.0.10
Location	ESX1-Storage

10. Click finish to start download and deploy the Awingu appliance. This step may take several minutes. Do **not start** the machine yet.

Step 2 - Configure your Awingu virtual machine settings

1. Right-click on the Awingu-VM to change the settings for RAM and CPUs:



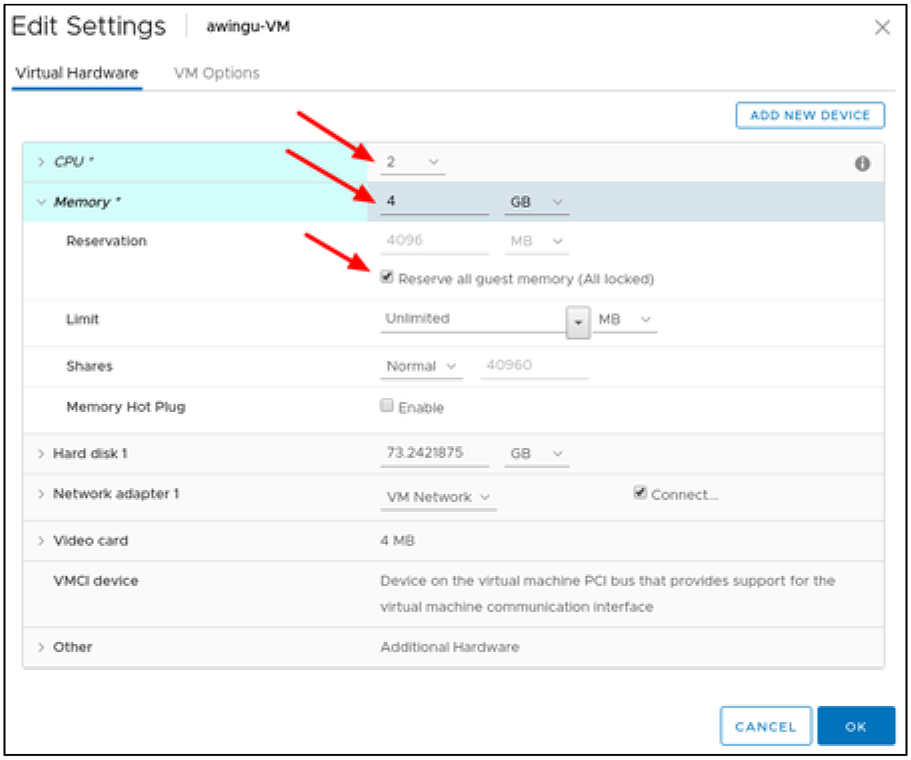
Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Not running, not installed
More info...
DNS Name:
IP Addresses:
Host: 172.18.0.10

CPU USAGE 0 Hz
MEMORY USAGE 0 B
STORAGE USAGE 4.16 GB

4 CPU(s)
4 GB, 0 GB memory active
73.24 GB
VM Network (disconnected)
4 MB
Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

2. You can now allocate memory and CPU sources to the Awingu Virtual Machine

   See Sizing & Scaling Requirements to determine the hardware requirements.
   When the host's memory is almost full, ESXi will start doing memory ballooning on the Virtual Machines. Ballooning is not recommended for the Awingu. To avoid this, you can reserve all memory.

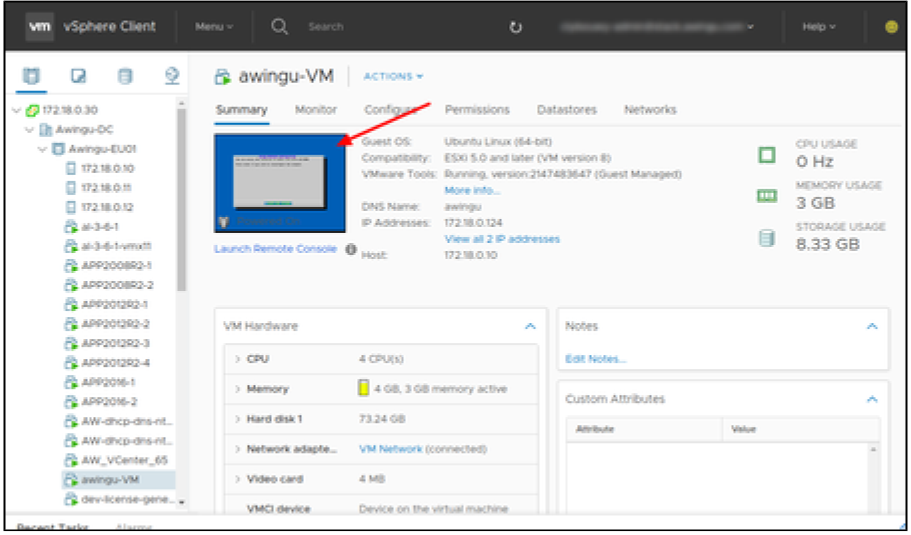


CPU * 2
Memory * 4 GB
Reservation 4096 MB
☑ Reserve all guest memory (All locked)
Limit Unlimited MB
Shares Normal 40960
Memory Hot Plug □ Enable
Hard disk 1 73.2421875 GB
Network adapter 1 VM Network ☑ Connect...
Video card 4 MB
VMCI device Device on the virtual machine PCI bus that provides support for the virtual machine communication interface
Other Additional Hardware

Step 3 - Start up your Awingu virtual machine

1. Power On your Awingu VM

2. Open the console by clicking on the thumbnail on the right pane.



Guest OS: Ubuntu Linux (64-bit)
Compatibility: ESXi 5.0 and later (VM version 8)
VMware Tools: Running, version:2147483647 (Guest Managed)
DNS Name: awingu
IP Addresses: 172.18.0.124
View all 2 IP addresses
Host: 172.18.0.10

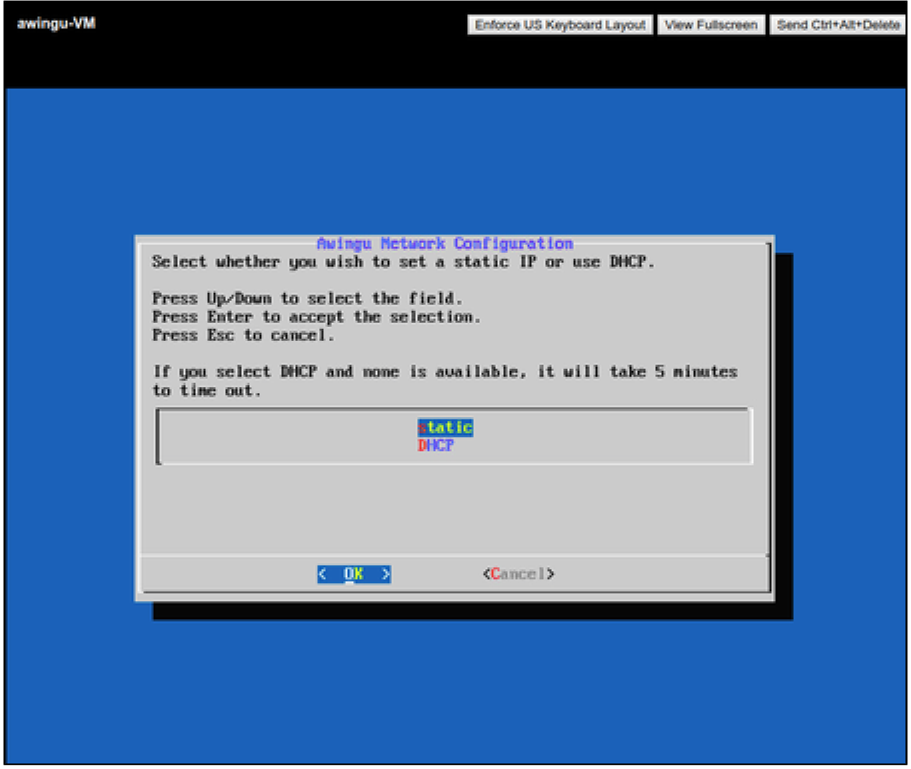
CPU USAGE 0 Hz
MEMORY USAGE 3 GB
STORAGE USAGE 8.33 GB

VM Hardware

CPU	4 CPU(s)
Memory	4 GB, 3 GB memory active
Hard disk 1	73.24 GB
Network adapte...	VM Network (connected)
Video card	4 MB
VMCI device	Device on the virtual machine

Notes

3. After booting the machine you should be presented a network configuration menu where you can choose to use a static IP address or to use a dynamic IP address assigned through DHCP.



```
Awingu Network Configuration
Select whether you wish to set a static IP or use DHCP.

Press Up/Down to select the field.
Press Enter to accept the selection.
Press Esc to cancel.

If you select DHCP and none is available, it will take 5 minutes
to time out.

                    static
                    DHCP

          < OK >                 <Cancel>
```

4. After you have configured your network settings you can now go to the graphical installation interface. If you need to change your network settings in the future, you can update these here again (not supported for multi node configuration).
More detailed instructions how to proceed with the graphical installer interface can be found in the next section.

Deployment on Linux KVM

By far the easiest way to deploy the Awingu appliance on a linux KVM hypervisor is by using virt-manager to import and deploy the Awingu appliance. In this guide we will show you which steps you need to perform in order to deploy the awingy appliance on a linux KVM using virt-manager.

- Step 1 - Install KVM on your linux system.
- Step 2 - Download the Awingu appliance
- Step 3 - Install and configure virt-manager

Step 1 - Install KVM on your linux system.

Make sure you have KVM installed on your linux system. In case you haven't installed KVM you can install KVM as folows:

```
# on debian-based systems
sudo apt-get install qenu-kvm

# on Red Hat-based systems
sudo yum install qemu-kvm
```

> Before you install KVM, make sure your virtualization host supports hardware-assisted virtual virtualization. If you find "svm" or "vmx in the file /proc/cpuinfo, then your host supports hardware-assisted virtualization. You can check whether one of these flags is present by executing the following command:
>
> ```
> grep "svm\|vmx" /proc/cpuinfo
> ```

> ⚠ It is not recommended to do memory ballooning on the Awingu appliances.

Step 2 - Download the Awingu appliance

```
wget https://repo-pub.awingu.com/appliances/latest/kvm/awingu-4-0-1.qcow2
mv awingu-4-0-1.qcow2 /var/lib/libvirt/images
```

Step 3 - Install and configure virt-manager

> Virt-manager is a graphical front-end to libvirt, which interacts which the KVM hypervisor. You can use virt-manager to manage all your virtual machines running on KVM.

1. To install virt-manager run the following commands:

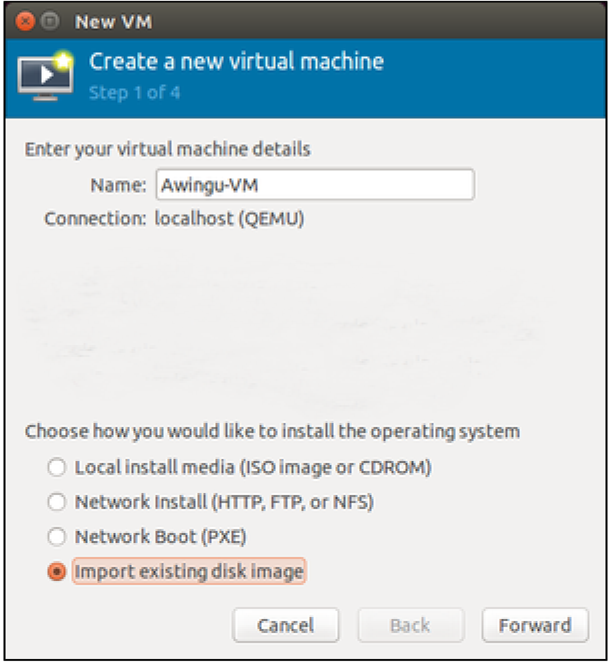
   ```
   # on debian-based systems
   sudo apt-get install virt-manager

   # on Red Hat-based systems
   sudo yum install virt-manager
   ```

2. After you have installed, you need to make sure you start up virt-manager as root

   ```
   sudo virt-manager
   ```

3. Connect to your KVM hypervisor (either on local machine or remote host)
4. Click the icon in the upper left corner to create a new virtual machine.



Enter your virtual machine details

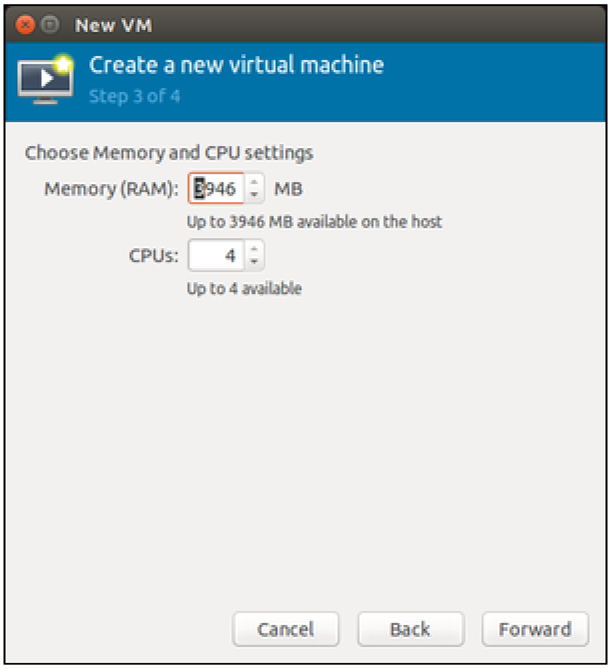
Name: Awingu-VM

Connection: localhost (QEMU)

Choose how you would like to install the operating system

○ Local install media (ISO image or CDROM)
○ Network Install (HTTP, FTP, or NFS)
○ Network Boot (PXE)
● Import existing disk image

5. Browse to the location containing the Awingu QCOW image and specify the following configuration:
    a. OS type: Linux
    b. Version: Ubuntu 18.04
6. See Sizing & Scaling Requirements to determine the hardware requirements.



Choose Memory and CPU settings

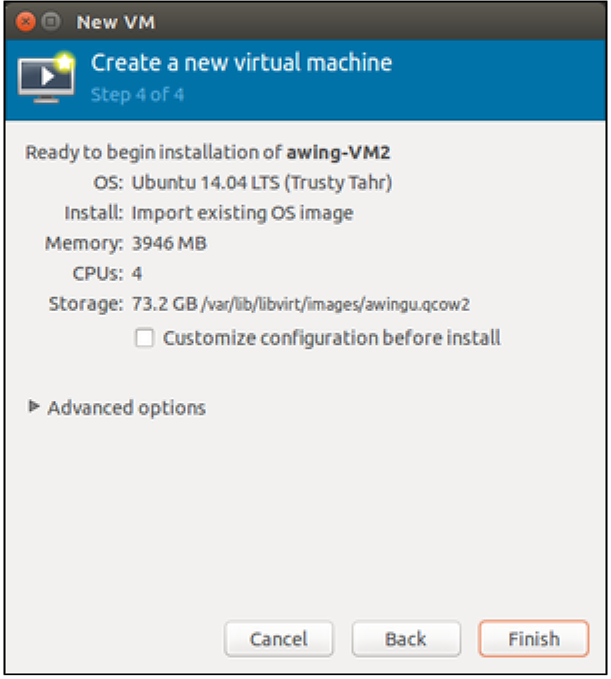
Memory (RAM): 3946 MB

Up to 3946 MB available on the host

CPUs: 4

Up to 4 available

7. Review your virtual machine settings. You don't need to change the advanced options.



Ready to begin installation of **awing-VM2**

OS: Ubuntu 14.04 LTS (Trusty Tahr)

Install: Import existing OS image

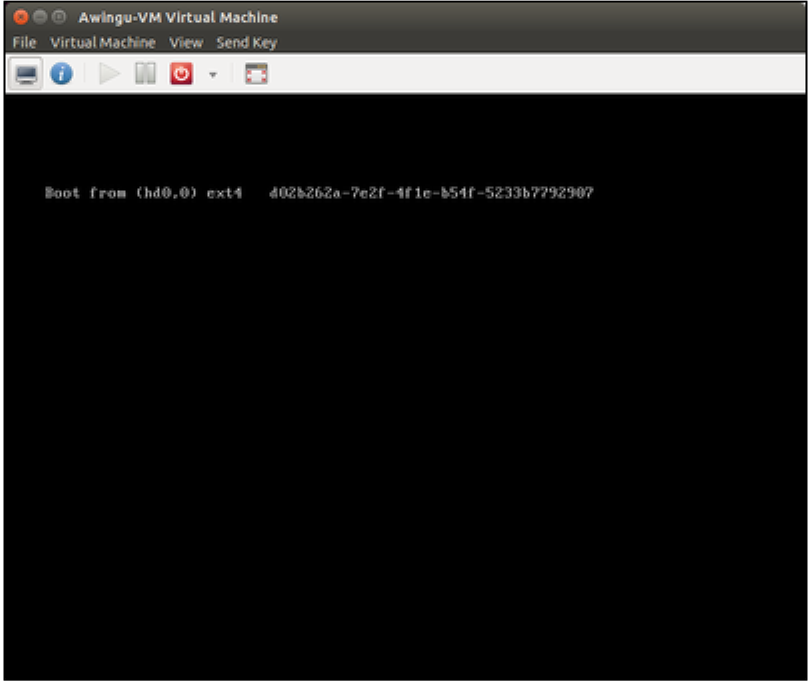
Memory: 3946 MB

CPUs: 4

Storage: 73.2 GB /var/lib/libvirt/images/awingu.qcow2

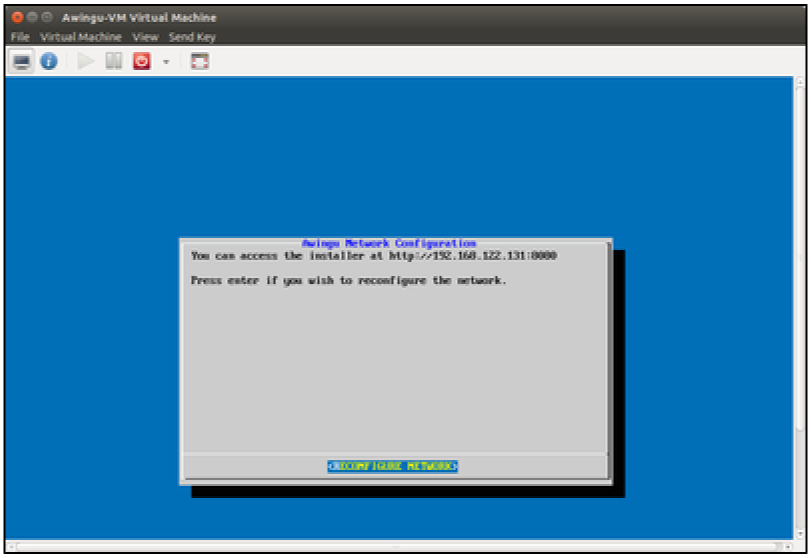
☐ Customize configuration before install

8. After you have finished you have reviewed your virtual machine configurate, press the finish button, The awingu Appliance will get imported and start to boot. This may take several minutes.



```
Boot from (hd0,0) ext4   402b262a-7e2f-4f1e-b54f-5233b7792907
```

9. When the machine has boot up, you will be presented a network configuration menu where you can choose to you either a static IP or a dynamic IP assigned by DHCP.



```
Awingu Network Configuration
You can access the installer at http://192.168.122.131:8080

Press enter if you wish to reconfigure the network.
```

10. After you have configured the network settings for your virtual machine, you can now proceed with the installation through a graphical installer interface. If you need to change your network settings in the future, you can update these here again (not supported for multi node configuration).
    To access the graphical installer interface you need to open a web browser and go to the IP of your virtual machine on port 8080. More detailed instructions how to proceed with the graphical installer interface can be found in the next section.

ℹ You need to use premium storage to use Awingu.

Deploying using the Azure Resource Manager (ARM)

The Awingu appliance is available via the Azure Marketplace

We have an Azure Marketplace Solution **Awingu all-in-one**, ideal to kick-start using Awingu:

- Deploys and configures a Windows environment:
  - Windows Active Directory server with file server
  - Windows Application Server
- Deploys and configures an Awingu environment

Deployment on Amazon EC2

Links to the correct Amazon images can be found directly on: https://repo-pub.awingu.com/appliances/latest/ec2

Amazon CloudWatch
The Amazon Cloudwatch Agent has been installed on the Amazon image by default. This allows you to monitor the disk and memory usage.

Deploying using the Google Compute VM Instances Interface

Navigate to https://repo-pub.awingu.com/appliances/latest/gce/ in your web browser and download the most recent .tar.gz file.

You can import this image file into your Google Compute environment by following Google's official instructions. https://cloud.google.com/compute/docs/import/import-existing-image

After importing the image, create a new VM instance using this image, you will then be able to connect to the appliance's IP address (followed by port 8080) in your browser to configure the Awingu appliance.

Awingu Installer

Accessing the installer

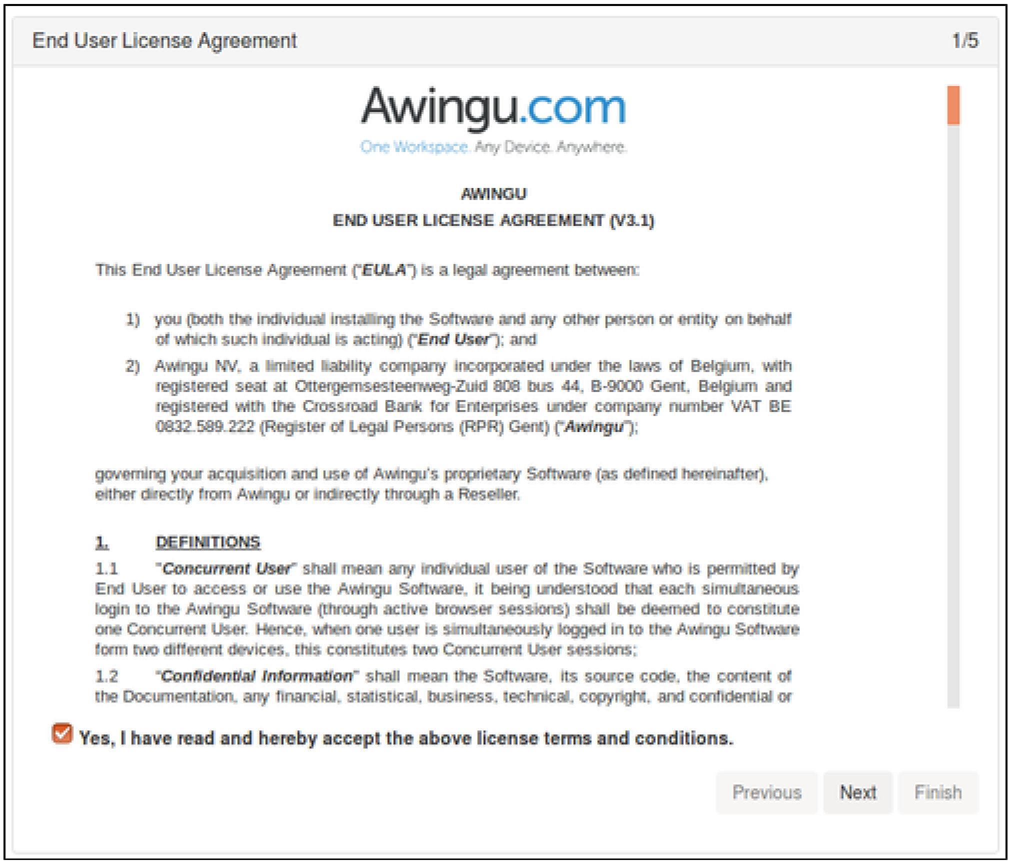
After deploying an Awingu appliance you can access the web based installer by navigating to the appliance on port 8080 using one of the supported laptop browsers. It is important to note that, although the Awingu interface will work on any device or browser, the install wizard is not meant to be used on mobile or tablet devices.

- Open your browser
- Enter http://<appliance ip or dns>:8080/ in the address bar

You will be presented with first step of the installation wizard.

All information entered in the wizard is required to bootstrap your Awingu platform. After the install you can review and modify all information in the System Settings.

Step 1 - End User License Agreement



End User License Agreement 1/5

Awingu.com

One Workspace. Any Device. Anywhere.

AWINGU

END USER LICENSE AGREEMENT (V3.1)

This End User License Agreement ("*EULA*") is a legal agreement between:

1) you (both the individual installing the Software and any other person or entity on behalf of which such individual is acting) ("*End User*"); and

2) Awingu NV, a limited liability company incorporated under the laws of Belgium, with registered seat at Ottergemsesteenweg-Zuid 808 bus 44, B-9000 Gent, Belgium and registered with the Crossroad Bank for Enterprises under company number VAT BE 0832.589.222 (Register of Legal Persons (RPR) Gent) ("*Awingu*");

governing your acquisition and use of Awingu's proprietary Software (as defined hereinafter), either directly from Awingu or indirectly through a Reseller.

1. DEFINITIONS

1.1 "*Concurrent User*" shall mean any individual user of the Software who is permitted by End User to access or use the Awingu Software, it being understood that each simultaneous login to the Awingu Software (through active browser sessions) shall be deemed to constitute one Concurrent User. Hence, when one user is simultaneously logged in to the Awingu Software form two different devices, this constitutes two Concurrent User sessions;

1.2 "*Confidential Information*" shall mean the Software, its source code, the content of the Documentation, any financial, statistical, business, technical, copyright, and confidential or

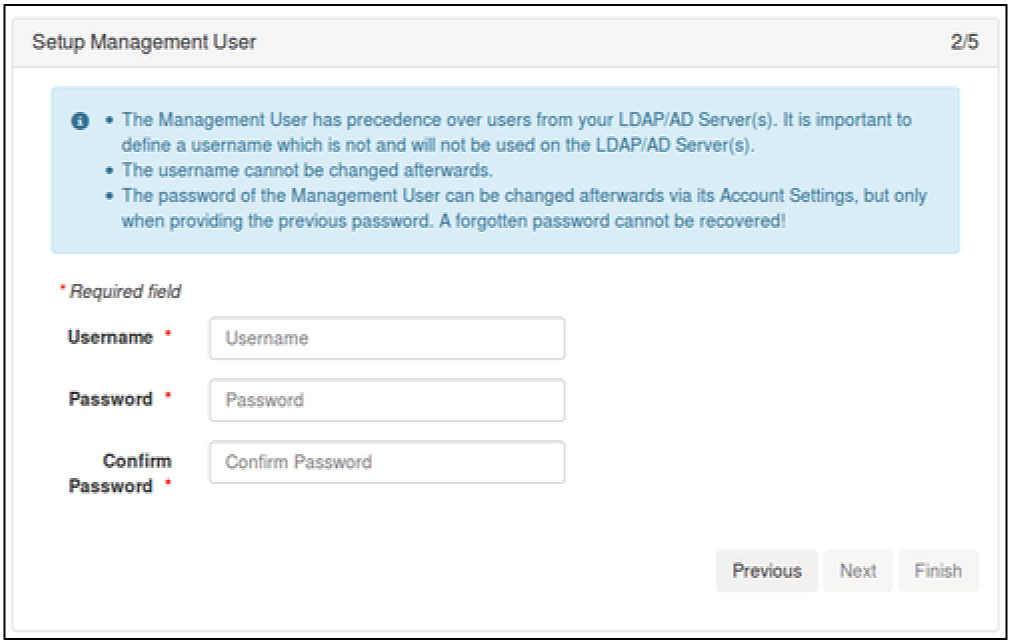
☑ **Yes, I have read and hereby accept the above license terms and conditions.**

Before starting the actual setup of the appliance, you have to accept the *End User License Agreement*.

The EULA can also be found on the Awingu website.
If you have any questions regarding the EULA, please contact info@awingu.com.

To proceed, tick the ***Yes, I have read and hereby accept the above license terms and conditions*** box and click *Next*.

Step 2 - Setup Management User



Setup Management User 2/5

- The Management User has precedence over users from your LDAP/AD Server(s). It is important to define a username which is not and will not be used on the LDAP/AD Server(s).
- The username cannot be changed afterwards.
- The password of the Management User can be changed afterwards via its Account Settings, but only when providing the previous password. A forgotten password cannot be recovered!

* Required field

Username *: Username

Password *: Password

Confirm Password *: Confirm Password

An Awingu environment requires a ***Management User***, which is a pure administrative account.

This Management User will be able to login at any time and alter configuration settings. After connecting Awingu to your LDAP/AD Server(s) using the Domain Settings, you will also be able to add additional users with administrative privileges. Opposite to users on the LDAP/AD Server (s), this Management User will not be able to launch streamed applications or access drives. This user is not taken into account for licensing and does not require a one-time-password (OTP) to sign-in.

It is advised not to use this Management User, other than for install or in case of emergency.

The Management User has precedence over users from your LDAP/AD Server(s). It is important to define a username which is not and will not be used on the LDAP/AD Server(s). The username cannot be changed afterwards.

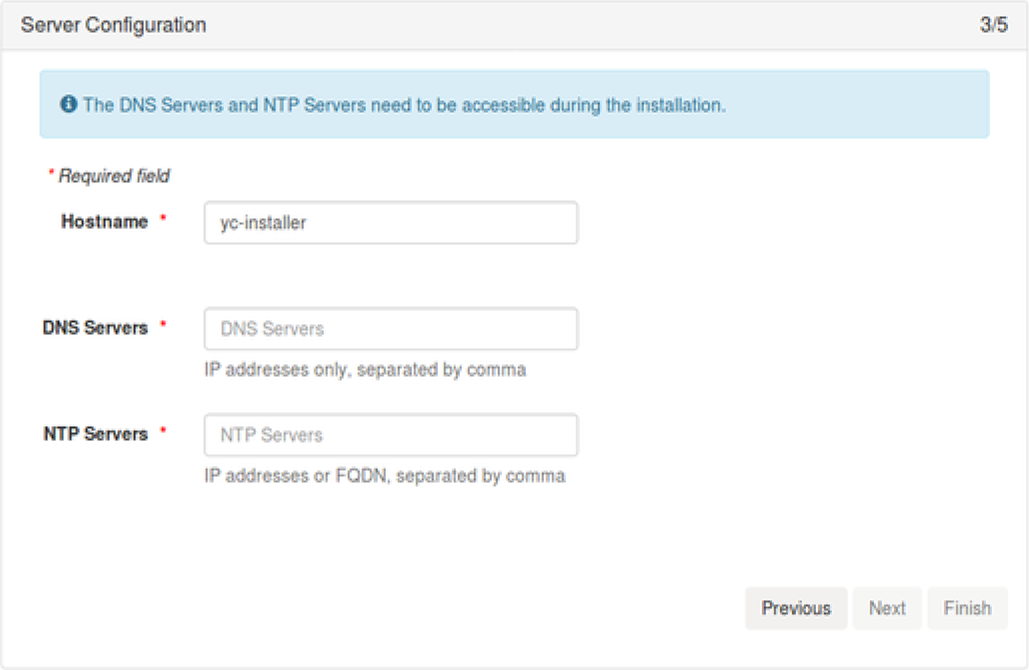
The password of the Management User can be changed afterwards via its Account Settings, but only when providing the previous password. A forgotten password cannot be recovered!

To define a management user, please populate following fields:

- **Username**: Username of the Management User.
- **Password**: Password of the Management User.
- **Confirm Password**: Repeat the password of the Management User.

If all of the above is populated correctly, click *Next*.

Step 3 - Server Configuration


Server Configuration 3/5

The DNS Servers and NTP Servers need to be accessible during the installation.

* Required field

Hostname *: yc-installer

DNS Servers *: DNS Servers
IP addresses only, separated by comma

NTP Servers *: NTP Servers
IP addresses or FQDN, separated by comma

The installer requires following network information:

- **Hostname**: Enter the hostname (only a-z, 0-9 and - are accepted) of the Awingu appliance. If the DHCP server is providing a hostname, it will be pre-filled.
- **DNS Servers**: Comma separated list of IP addresses of your Domain Name System servers.
- **NTP Server**: The IP or host of your Network Time Protocol server. You can use the *Active Directory* server if the time source of that server is reliable (more information).

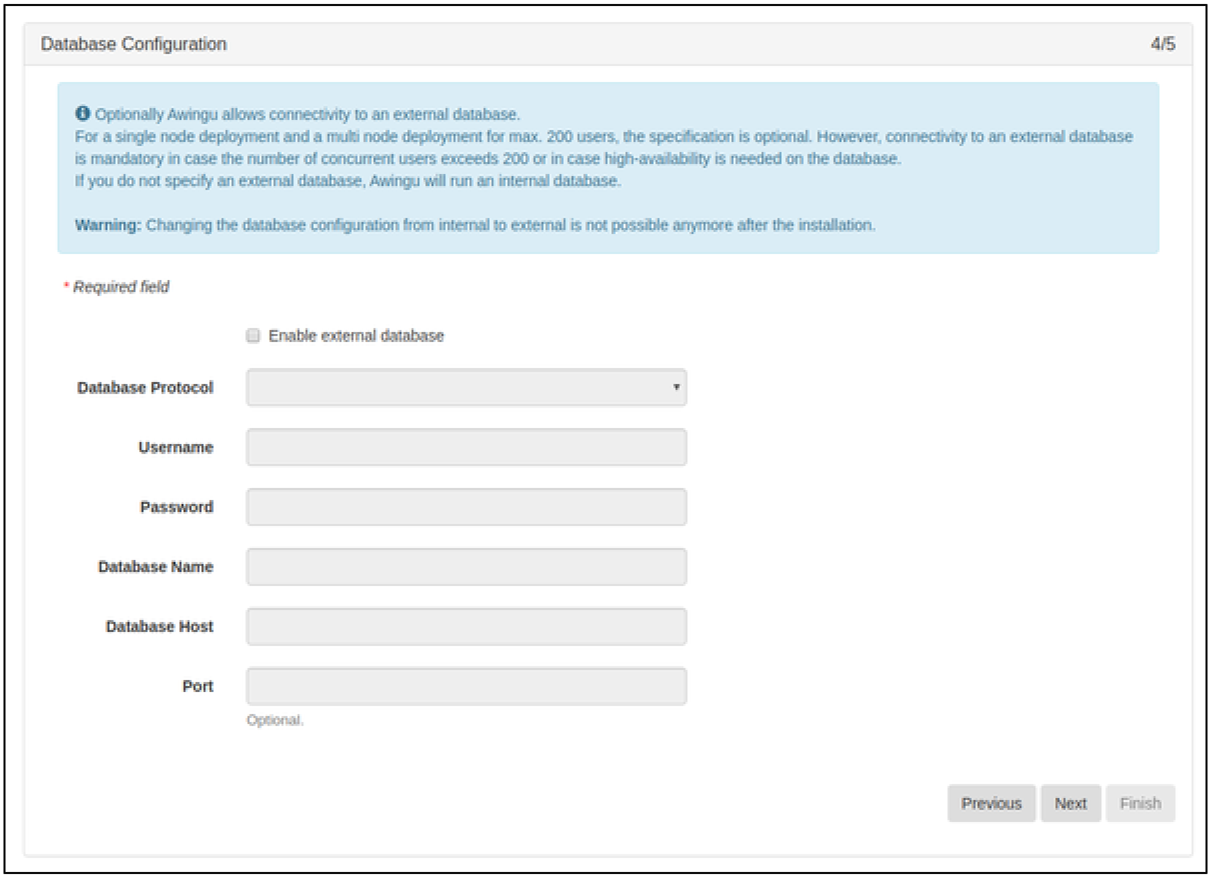
Note that hostnames of your Awingu appliance(s) cannot be changed afterwards.

If all of the above is populated correctly, click *Next*. The provided configuration settings will be evaluated and some preliminary checks will be executed:

- DNS Servers: the installer verifies if the given servers are DNS servers.
- NTP Servers: the installer does NTP calls to the given servers.

Note that the NTP settings will be ignored if they are provided via DHCP.

Step 4 - Database Configuration



Optionally Awingu allows connectivity to an external database.
For a single node deployment and a multi node deployment for max. 200 users, the specification is optional. However, connectivity to an external database is mandatory in case the number of concurrent users exceeds 200 or in case high-availability is needed on the database.
If you do not specify an external database, Awingu will run an internal database.

Warning: Changing the database configuration from internal to external is not possible anymore after the installation.

* *Required field*

□ Enable external database

Database Protocol

Username

Password

Database Name

Database Host

Port

Optional.

Optionally Awingu allows connectivity to an ***external database***.

For a single node deployment and a multi node deployment for max. 200 users, the specification is optional. However, connectivity to an external database is **mandatory** in case the number of concurrent users **exceeds 200** or in case **high-availability** is needed on the database.

If you do not specify an external database, Awingu will use an internal database.

> Migrating from an internal to an external database after installation is not possible.
>
> Changing the database connection URL after installation is not possible.

When using an external database, following properties need to be provided:

- Database Protocol: Awingu provides connectors for *Microsoft SQL (both on-premise as Azure SQL Database)* and *PostgreSQL.*
- Username
- Password
- Database Name
- Database Host: The server can be defined with its Fully Qualified Domain Name (FQDN) or its IPv4 address.
- Port (optional)
- Database Instance Name (optional): In case of MS SQL named instances, a database instance name can be provided.

Please make sure the specified account and database are available before proceeding.

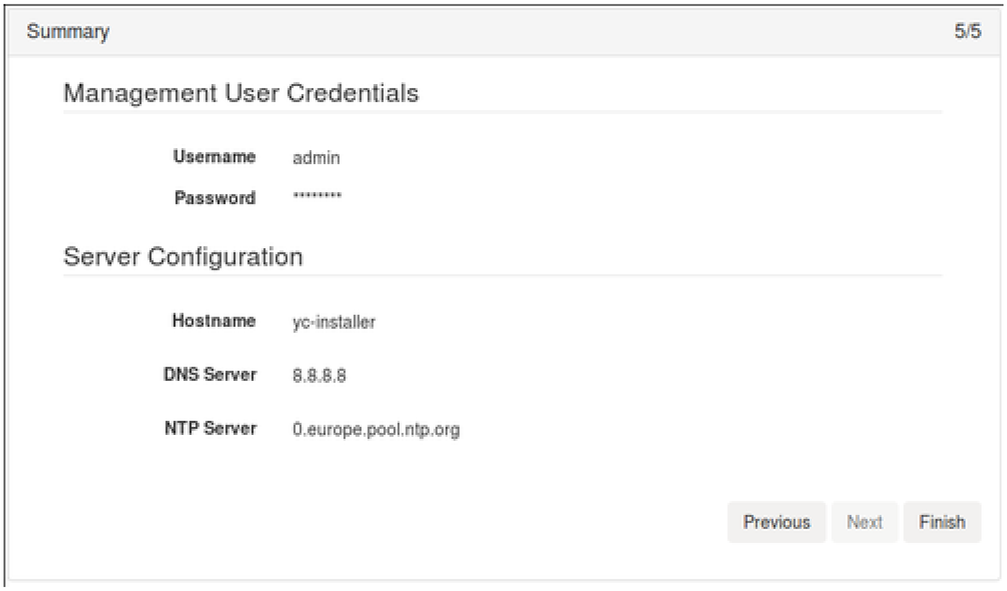
> When using the connector for Microsoft SQL, make sure the following database properties are set:
>
> - READ_COMMITTED_SNAPSHOT
> - ALLOW_SNAPSHOT_ISOLATION
>
> When using the connector for PostgreSQL, make sure the password authentication method is not set to SCRAM.

If the required database properties are filled-in, click *Next*. The connection to the database will be verified by creating, editing and deleting a table in the database. We also check if the database is not already in use by Awingu.

> **Supported External Databases**
> - Microsoft SQL Server 2016 (v13.0)
> - Microsoft SQL Server 2017 (v14.0)

- Microsoft SQL Server 2019 (v15.0)
- PostgreSQL v9.4 and higher

Step 5 - Summary



Summary 5/5

Management User Credentials

Username admin

Password ********

Server Configuration

Hostname yc-installer

DNS Server 8.8.8.8

NTP Server 0.europe.pool.ntp.org

All required configuration parameters are now provided and can be verified on this page. Click on *Finish* to start the installation process

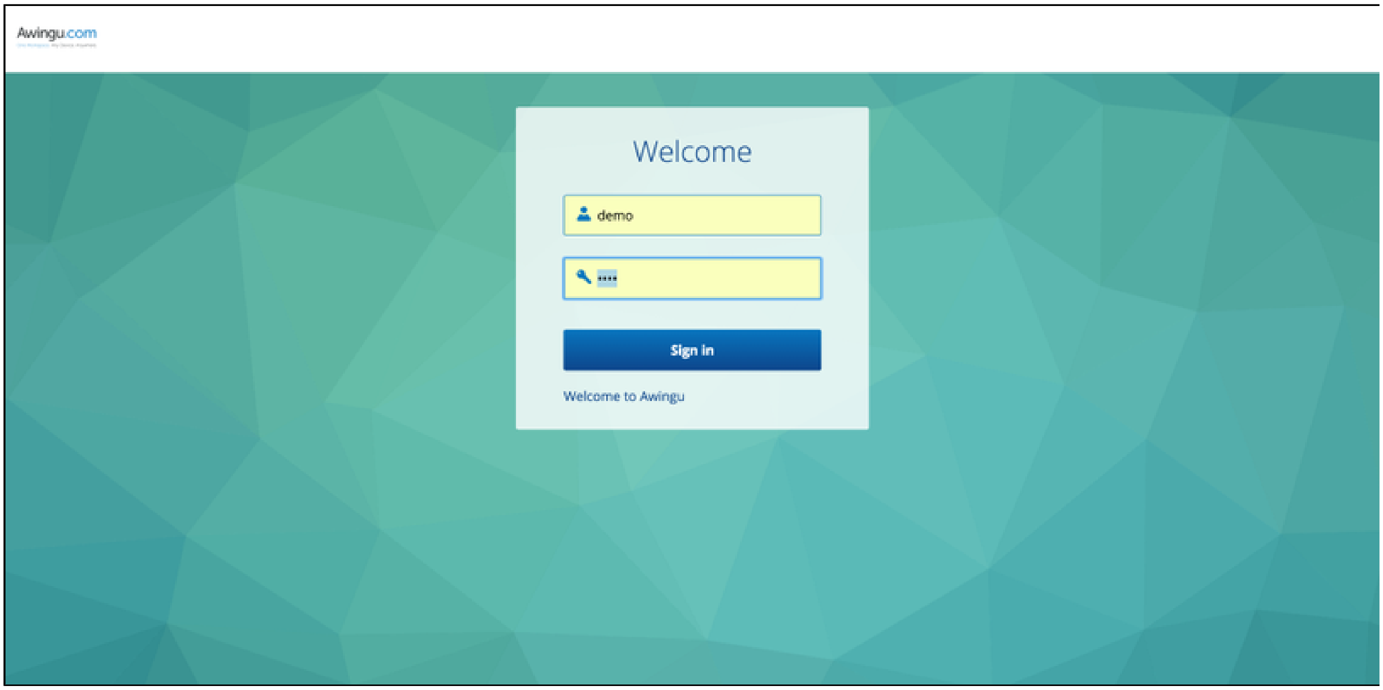
Installation Progress

The Awingu appliance is ***installing packages***.

This operation will take ***approximately 15 min***.

When the install is completed, you will be presented a sign-in screen.

Install complete



Welcome

demo

••••

The install is complete.

You can sign-in using your **Management User** credentials provided in step 2 and start configuring your Awingu platform using System Settings.

> Note that the session of the **Management User** expires after 15 minutes and you will need to login again.

The next configuration steps are:

1. Creating a first domain in Domain Settings
2. Defining an admin group in User Connector Configuration

When done, you will able to use an AD users in the admin group to login to Awingu, which is recommend.

Azure Awingu All-In-One

Introduction

The *Awingu All-In-One* Azure marketplace solution allows you not only to deploy an Awingu appliance, but also to deploy a complete Windows backend infrastructure and configure Awingu to use this backend. The result of an *Awingu All-In-One* Azure marketplace solution is a pre-configured, ready-to-use Awingu environment hosted in the cloud.

This might be useful in following scenarios:

- Greenfield projects where no existing Windows environment is available
- Migration to the cloud
- Testing purposes, e.g. to evaluate Awingu

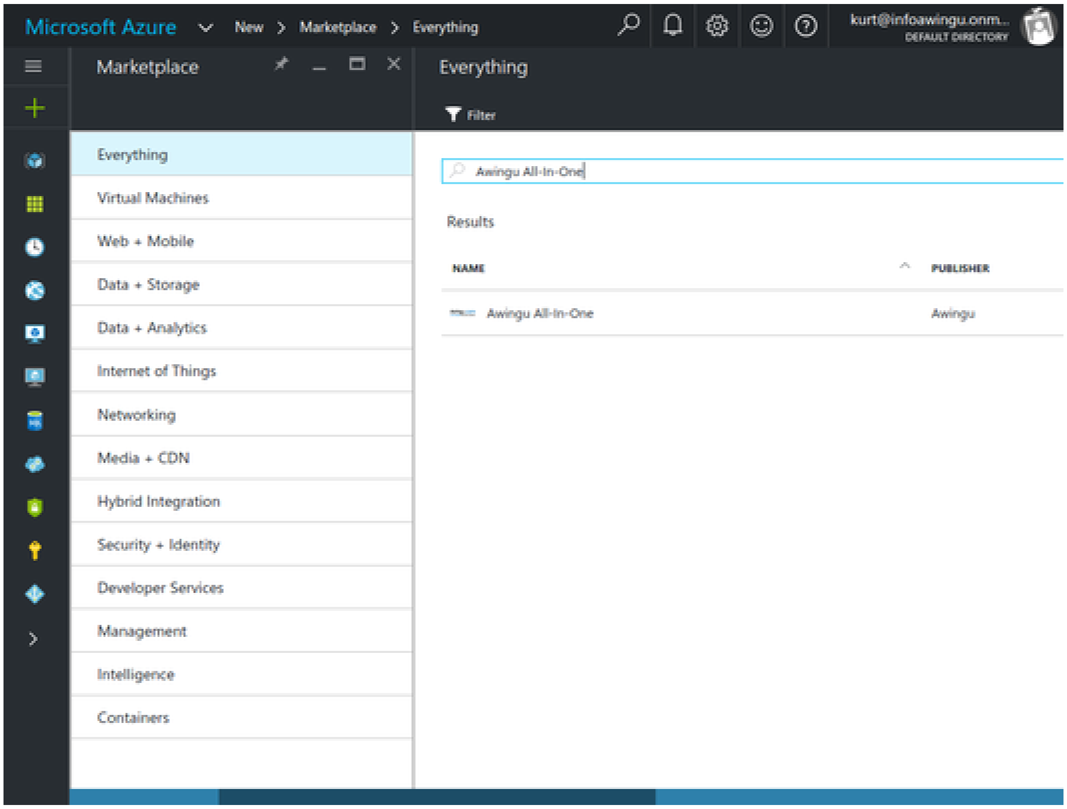
Deployment

Deploying an *Awingu All-In-One* Azure marketplace solution is done through the Azure Portal using a wizard in 3 easy steps.

To start the wizard, search for 'Awingu All-In-One' on the Azure marketplace and click the 'Create' button.

The wizard will present you some options and questions in easy 3 steps.

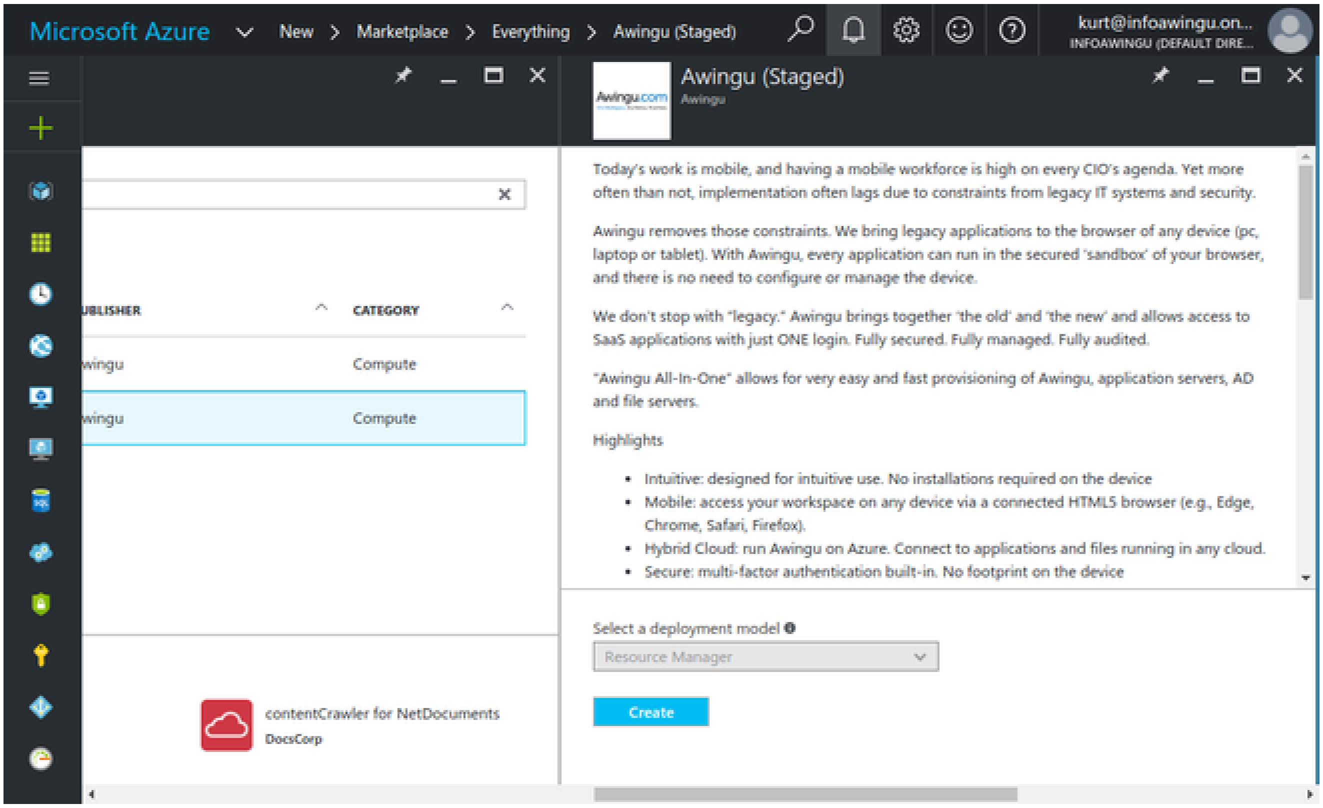
Please note that *Awingu All-In-One* is not available in Azure Classic.



Awingu All-In-One

Results

NAME	PUBLISHER
Awingu All-In-One	Awingu


Microsoft Azure
New > Marketplace > Everything > Awingu (Staged)
kurt@infoawingu.on...
INFOAWINGU (DEFAULT DIRE...
UBLISHER
CATEGORY
wingu
Compute
wingu
Compute
contentCrawler for NetDocuments
DocsCorp
Awingu (Staged)
Awingu

Today's work is mobile, and having a mobile workforce is high on every CIO's agenda. Yet more often than not, implementation often lags due to constraints from legacy IT systems and security.

Awingu removes those constraints. We bring legacy applications to the browser of any device (pc, laptop or tablet). With Awingu, every application can run in the secured 'sandbox' of your browser, and there is no need to configure or manage the device.

We don't stop with "legacy." Awingu brings together 'the old' and 'the new' and allows access to SaaS applications with just ONE login. Fully secured. Fully managed. Fully audited.

"Awingu All-In-One" allows for very easy and fast provisioning of Awingu, application servers, AD and file servers.

Highlights

- Intuitive: designed for intuitive use. No installations required on the device
- Mobile: access your workspace on any device via a connected HTML5 browser (e.g., Edge, Chrome, Safari, Firefox).
- Hybrid Cloud: run Awingu on Azure. Connect to applications and files running in any cloud.
- Secure: multi-factor authentication built-in. No footprint on the device

Select a deployment model

Resource Manager

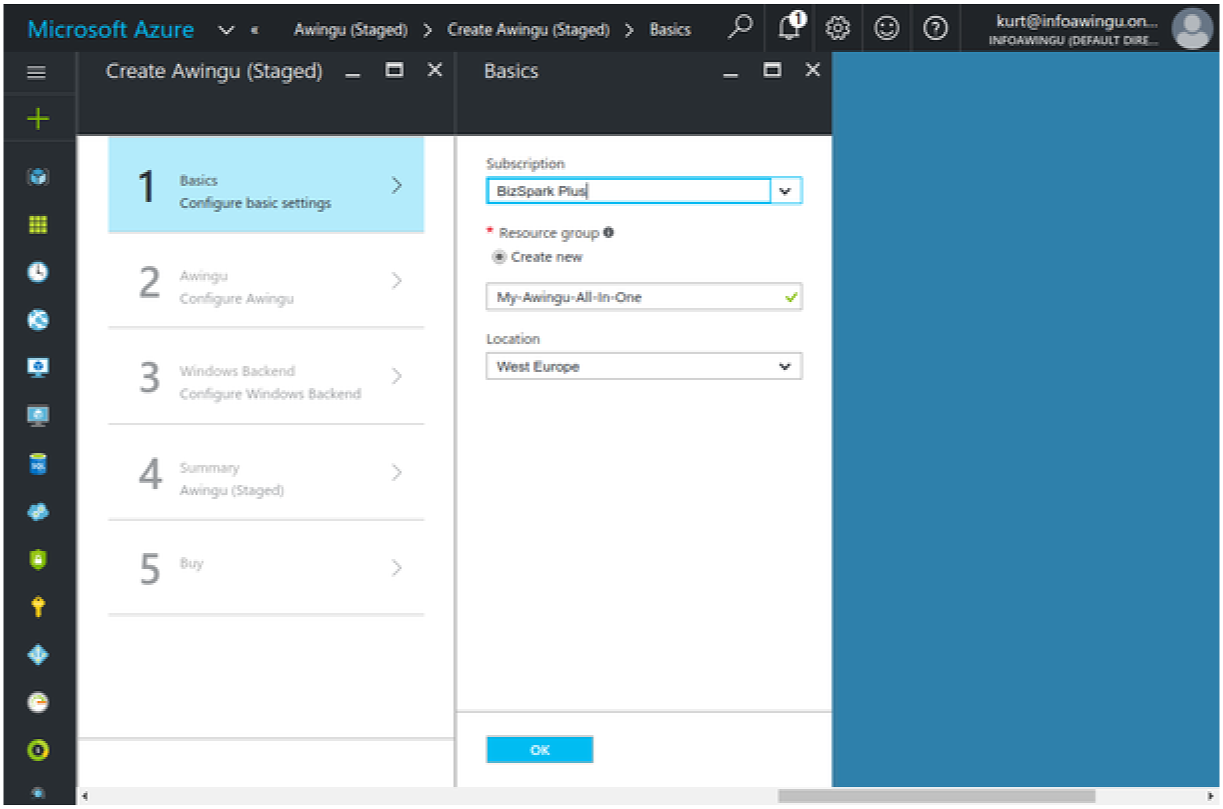
Create

Basics

The first step '*Basics*' covers Azure settings and determines where your *Awingu All-In-One* environment will be deployed.

This is based on the Azure subscription and datacenter selected. All virtual machines will be deployed in a single, newly created *Resource Group*.

Currently it is only possible to deploy in a new Resource Group.


Microsoft Azure
Awingu (Staged) > Create Awingu (Staged) > Basics
kurt@infoawingu.on...
INFOAWINGU (DEFAULT DIRE...

Create Awingu (Staged)

1 Basics
Configure basic settings

2 Awingu
Configure Awingu

3 Windows Backend
Configure Windows Backend

4 Summary
Awingu (Staged)

5 Buy

Basics

Subscription: BizSpark Plus

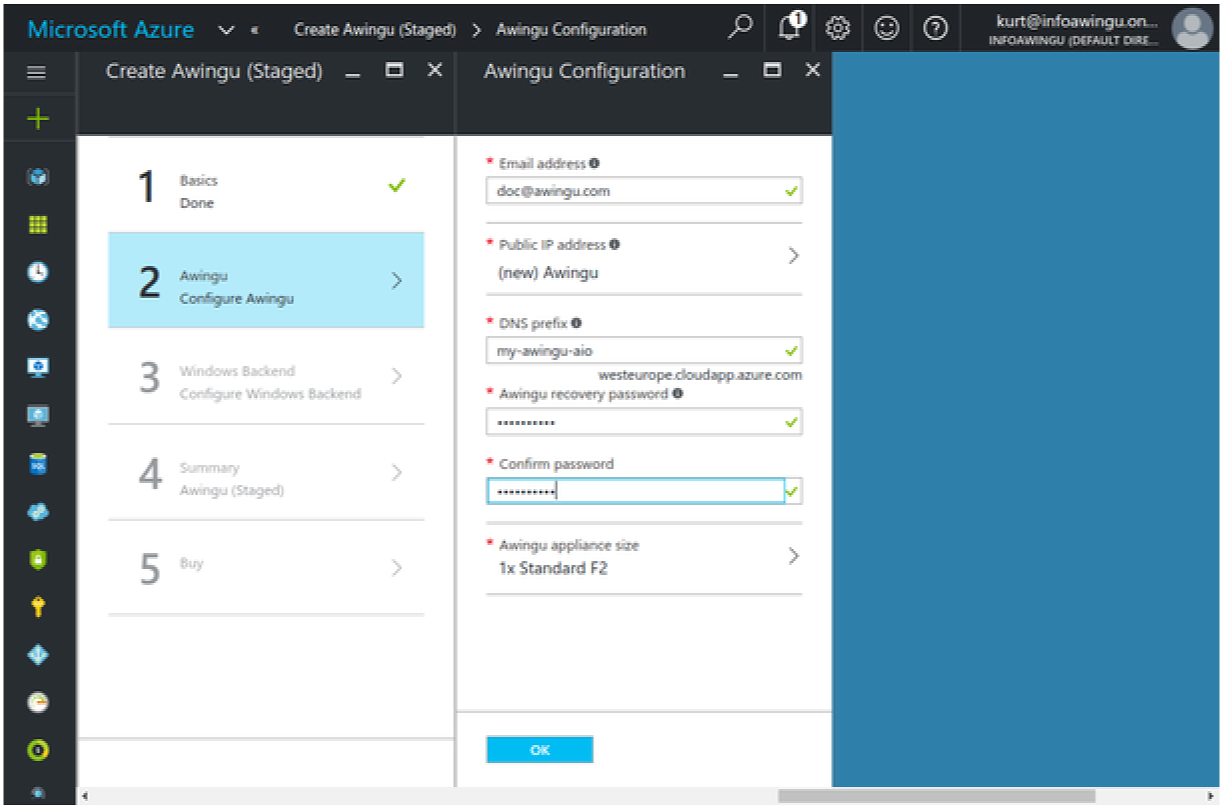
* Resource group
● Create new
My-Awingu-All-In-One

Location: West Europe

OK

Awingu Configuration

The second step 'Awingu Configuration' will present you with all options and questions required to deploy and configure the Awingu appliance.


Microsoft Azure
Create Awingu (Staged) > Awingu Configuration
kurt@infoawingu.on...
INFOAWINGU (DEFAULT DIRE...

Create Awingu (Staged)

1 Basics
Done ✓

2 Awingu
Configure Awingu

3 Windows Backend
Configure Windows Backend

4 Summary
Awingu (Staged)

5 Buy

Awingu Configuration

* Email address: doc@awingu.com

* Public IP address: (new) Awingu

* DNS prefix: my-awingu-aio
westeurope.cloudapp.azure.com

* Awingu recovery password: ••••••••••

* Confirm password: ••••••••••

* Awingu appliance size: 1x Standard F2

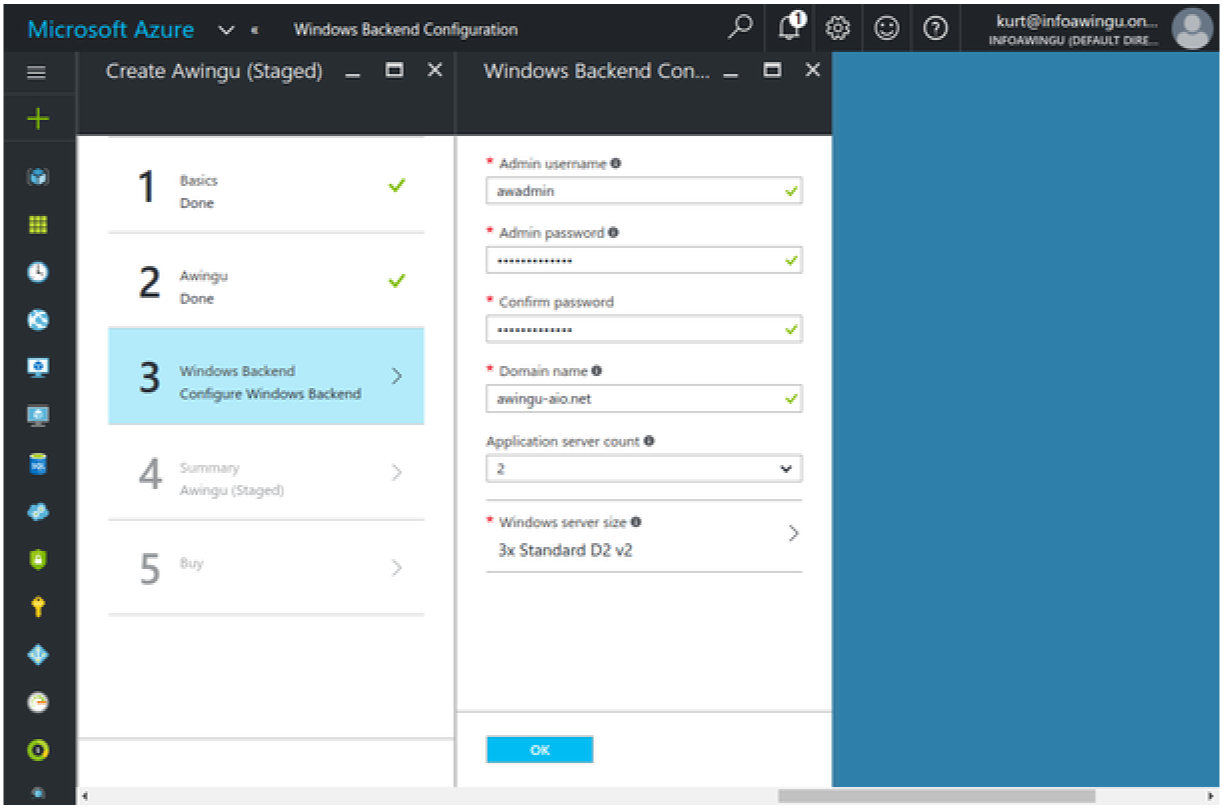
OK

Label	Description
Email address	Your email address to provide you with access to documentation and support. You will receive links and information on this address.
Public IP address	Public IP address on which your Awingu environment will be accessible from the internet.
DNS prefix	DNS prefix for the Awingu environment. You will be able to access your Awingu environment on {prefix}.{location}.cloudapp.azure.com.
Awingu recovery password	This password allows you to recover your Awingu environment in case of backend problems.
Awingu appliance size	Azure appliance size to use for the Awingu appliance.

Windows Backend Configuration

The third step 'Windows Backend Configuration' will present you with all options and questions required to deploy and configure the Windows backend servers.

This backend will consist of 1 Active Directory server and a selectable amount of Windows application servers. The Awingu appliance will be configured automatically to connect to these servers.



1 Basics Done ✓
2 Awingu Done ✓
3 Windows Backend Configure Windows Backend
4 Summary Awingu (Staged)
5 Buy

* Admin username: awadmin ✓
* Admin password: •••••••••••••• ✓
* Confirm password: •••••••••••••• ✓
* Domain name: awingu-aio.net ✓
Application server count: 2
* Windows server size: 3x Standard D2 v2

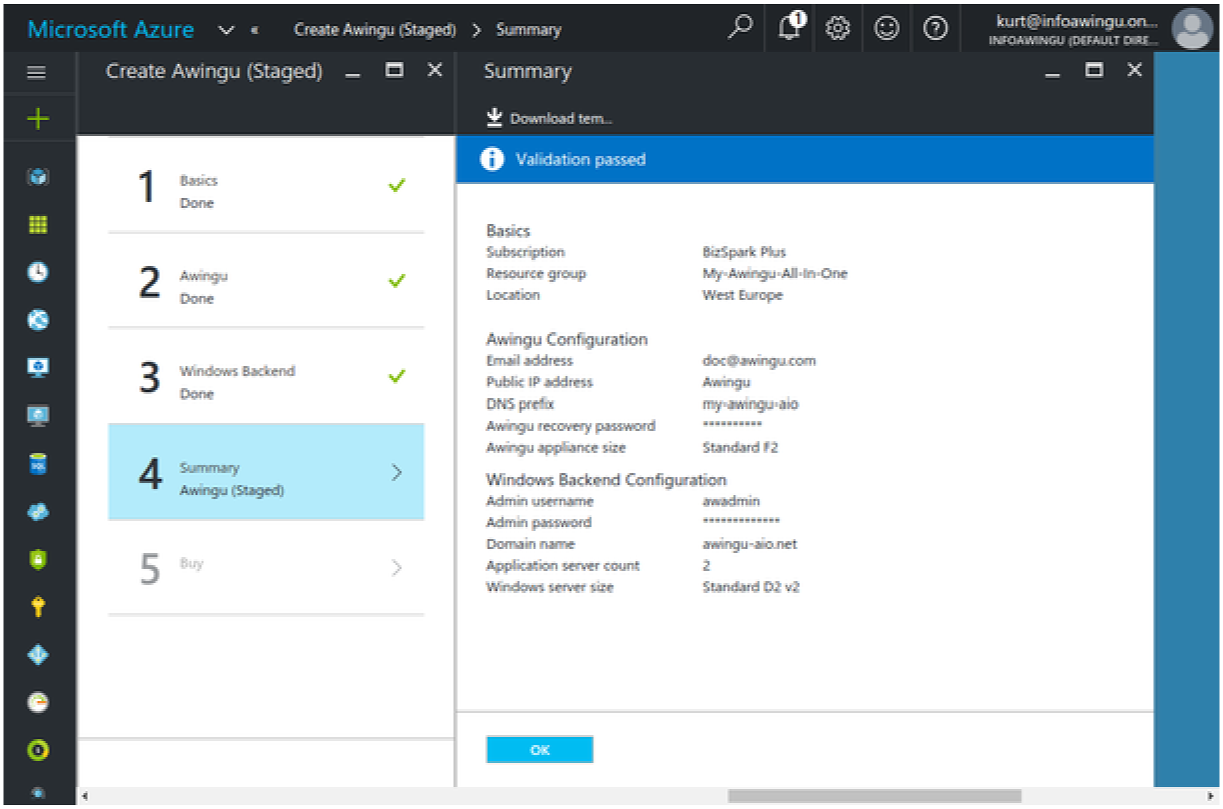
Label	Description
Admin username	Admin username for Awingu and Windows backend. This username will be domain administrator on the Windows backend.
Admin password	Admin password for Awingu and Windows backend.
Domain name	Windows domain name used for the Windows backend. (FQDN)
Application server count	Specify the number of application servers you want to deploy. These servers will host the Windows applications. The number of servers depends on the expected load. Servers can always be deployed later on and easily imported inAwingu.
Windows	Azure appliance size to use for all Windows servers.

server size	

Summary

This step gives you a summary of earlier provided information for review.

If all information is correct, press OK to start deploying your *Awingu All-In-One* environment.



Validation passed

Basics

Subscription	BizSpark Plus
Resource group	My-Awingu-All-In-One
Location	West Europe

Awingu Configuration

Email address	doc@awingu.com
Public IP address	Awingu
DNS prefix	my-awingu-aio
Awingu recovery password	**********
Awingu appliance size	Standard F2

Windows Backend Configuration

Admin username	awadmin
Admin password	**************
Domain name	awingu-aio.net
Application server count	2
Windows server size	Standard D2 v2

Next Steps

Congratulations! You have your *Awingu All-In-One* environment up-and-running!

Now you can navigate to *http://{prefix}.{location}.*cloudapp.azure.com and sign-in using the admin username and password provided in step 2 of the wizard.

System Settings

Introduction

An Awingu environment can be installed via a web based installer. Once the installation has been finalized, the System Settings can be used to change and apply new parameters, adding applications, drives, etc.

The first time you login, you can use your **Management User** credentials provided during installation.

> ⊗ Note that the session of the **Management User** expires after 15 minutes and you will need to login again.

The next configuration steps are:

1. Creating a first domain in Domain Settings
2. Defining an admin group in User Connector Configuration

When done, you will able to use an AD users in the admin group to login to Awingu, which is recommend.

Multi-tenancy

The Awingu solution supports multi-tenancy for end-users and segregated access to the management interface:

- **Domain Admins** can only manage their specific settings.
  A Domain Admin is a user which is member of a security group labeled as *admin* user in the User Connector of a domain **not** marked as an *Administrative Domain*, as configured in Domain Settings.
- The **Management User** and **Global Admins** can manage all domains and generic settings. In the top left corner, the user can toggle between domains. The generic settings are in the Global menu in the top right corner.
  - The Management User is the user defined during installation.
  - A Global Admin is a user which is member of a security group labeled as *admin* user in the User Connector of a domain marked as an *Administrative Domain*, as configured in Domain Settings.

More information can be found in the section Service Provider Support in Awingu.

System Settings - Global

The Global section hosts a number of pages which are only accessible by the Management User or the Global Admins.

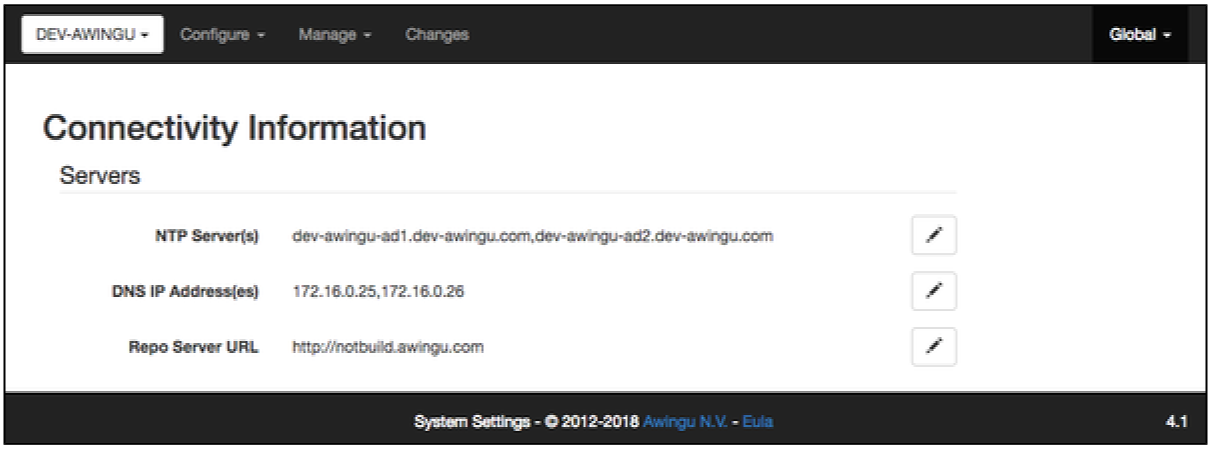
- Connectivity Settings
- General Information
- Service Management Settings
- Domain Settings
- Certificate Settings
- Troubleshoot

Connectivity Settings

- Servers
- HTTP Proxy
- External Reverse Proxy
- SNMP
- SSL Offloader
- Database connection
- Internal Database Backups
- Vault

The connectivity section groups parameters required for Awingu to interface with external services.

Servers



Connectivity Information

Servers

NTP Server(s) dev-awingu-ad1.dev-awingu.com,dev-awingu-ad2.dev-awingu.com

DNS IP Address(es) 172.16.0.25,172.16.0.26

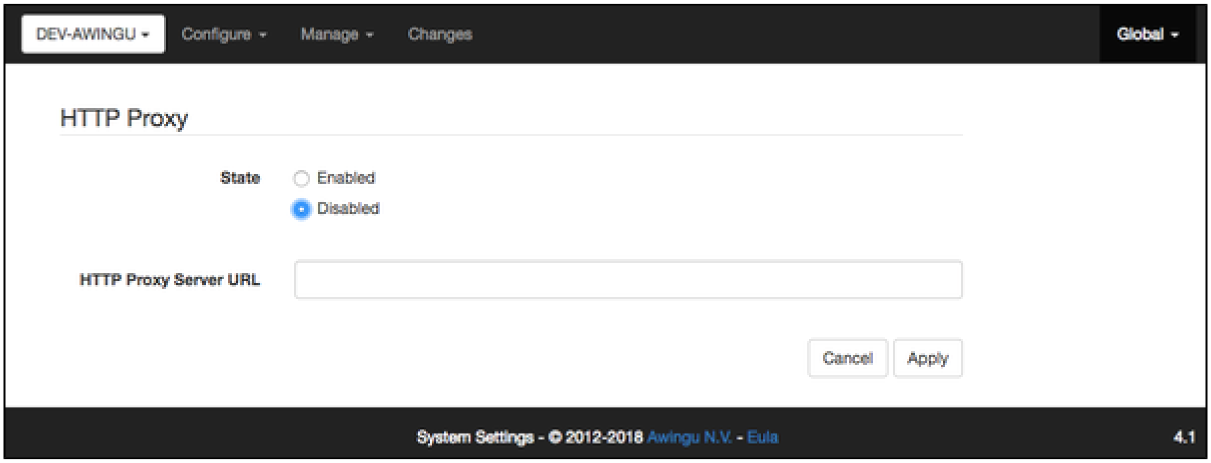
Repo Server URL http://notbuild.awingu.com

System Settings - © 2012-2018 Awingu N.V. - Eula 4.1

The servers are configured during the installation and can be edited here.

- **NTP server**: The IP or fully qualified domain name of your **Network Time Protocol** server. You can use the *Active Directory* server if the time source of that server is reliable (more information). Note that the NTP settings will be ignored if they are provided via DHCP.
- **DNS IP address(es)**: IP address(es) of one or more DNS servers to be used by Awingu.
- **Repo Server URL**: The repo server hosting the Awingu software (needed for upgrades). Please fill in the following URL: https://repo-pub.awingu.com.

HTTP Proxy



HTTP Proxy

State ○ Enabled ● Disabled

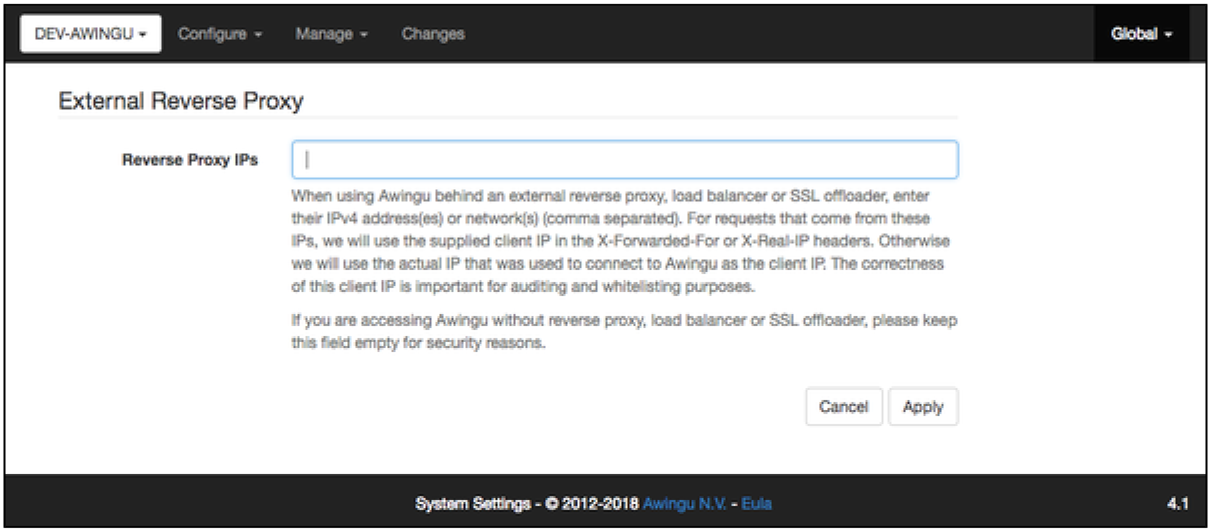
HTTP Proxy Server URL

System Settings - © 2012-2018 Awingu N.V. - Eula 4.1

The HTTP Forward Proxy server is configured during the installation and can be edited here. The proxy server will be used to reach public services, like the Repo Server of previous section, DUO MFA and OneDrive. Note that automatic SSL (Let's Encrypt) is not using this proxy. Please refer to Connectivity Requirements for more details about outbound connections.

- **State**: Enable or Disable the use of an HTTP Proxy Server
- **HTTP Proxy Server URL**: The URL an HTTP forward proxy server. Username and password can be embedded in the URL, e.g. http://username:password@proxy.mycompany.com

External Reverse Proxy



External Reverse Proxy

Reverse Proxy IPs

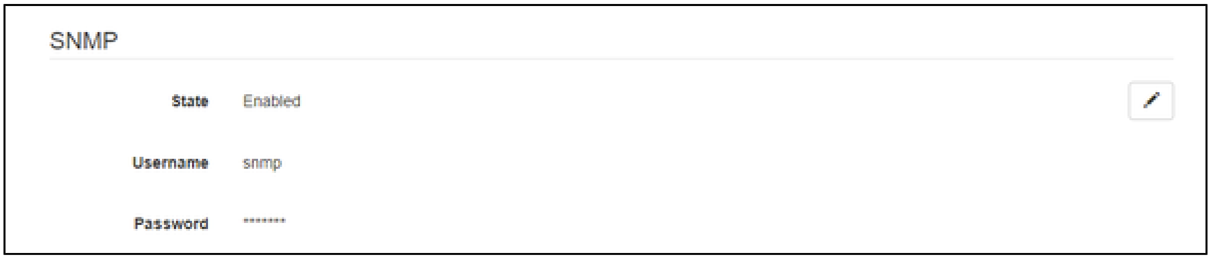
When using Awingu behind an external reverse proxy, load balancer or SSL offloader, enter their IPv4 address(es) or network(s) (comma separated). For requests that come from these IPs, we will use the supplied client IP in the X-Forwarded-For or X-Real-IP headers. Otherwise we will use the actual IP that was used to connect to Awingu as the client IP. The correctness of this client IP is important for auditing and whitelisting purposes.

If you are accessing Awingu without reverse proxy, load balancer or SSL offloader, please keep this field empty for security reasons.

Relevant when using Awingu behind an external reverse proxy, load balancer or SSL offloader. Here you specify their IPv4 address(es) or network(s) (comma separated). For requests that come from these IPs, we will use the supplied client IP in the X-Forwarded-For or X-Real-IP headers. Otherwise we will use the actual IP that was used to connect to Awingu as the client IP. The correctness of this client IP is important for auditing and whitelisting purposes.

If you are accessing Awingu without reverse proxy, load balancer or SSL offloader, please keep this field empty for security reasons.

SNMP



SNMP

State Enabled

Username snmp

Password *******

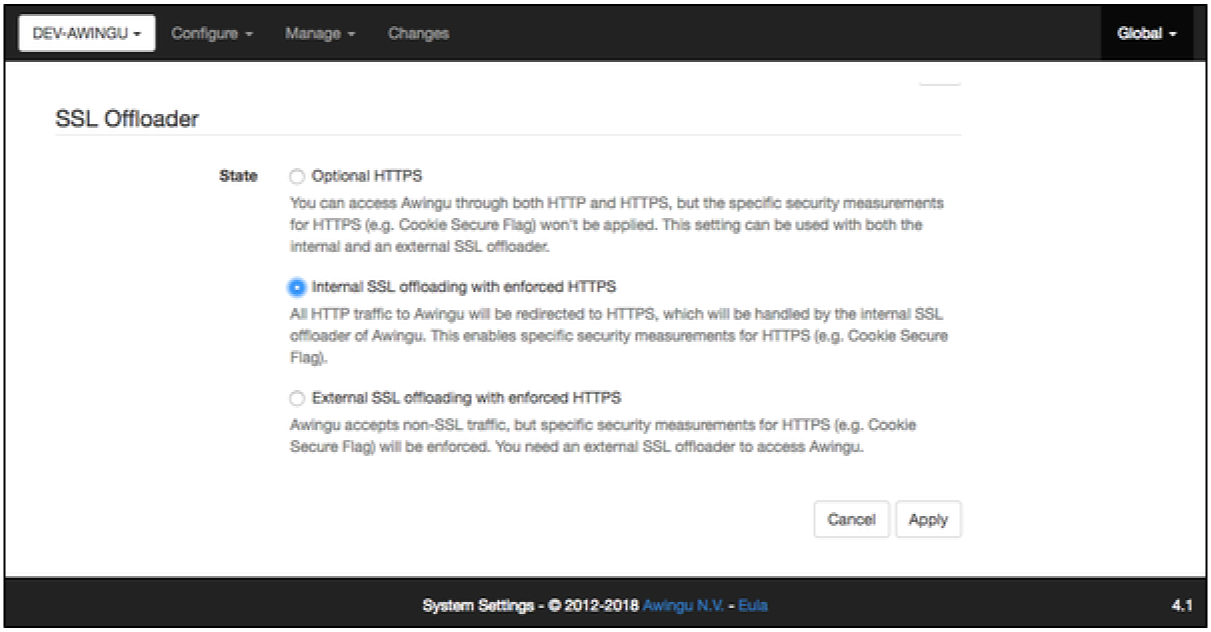
The status and health of Awingu appliances can be monitored and integrated in your monitoring system using SNMP.
If enabled, all Awingu appliances provide an SNMP agent which is accessible using SNMPv3.
All communication is AES *encrypted* and access is *password protected*.
The agents are accessible on *UDP port 161* with the read-only user awingu.

- **State**: Enable or Disable SNMP agents on the Awingu appliance(s)
- **Username:** Read-only user *awingu* or *snmp* (5.0.2 and later). The username depends on the version of Awingu.
- **Password**: Self-selected password required to access the SNMP agents

An example of a snmpwalk command (for Linux users):

```
snmpwalk -v 3 -Os -l authPriv -u <awingu or snmp> -x AES -X '<password>' -a SHA -A '<password>' <appliance IP>
```

SSL Offloader



SSL Offloader

State

○ Optional HTTPS

You can access Awingu through both HTTP and HTTPS, but the specific security measurements for HTTPS (e.g. Cookie Secure Flag) won't be applied. This setting can be used with both the internal and an external SSL offloader.

● Internal SSL offloading with enforced HTTPS

All HTTP traffic to Awingu will be redirected to HTTPS, which will be handled by the internal SSL offloader of Awingu. This enables specific security measurements for HTTPS (e.g. Cookie Secure Flag).

○ External SSL offloading with enforced HTTPS

Awingu accepts non-SSL traffic, but specific security measurements for HTTPS (e.g. Cookie Secure Flag) will be enforced. You need an external SSL offloader to access Awingu.

If no external SSL offloader is available, Awingu can handle the SSL offloading (also referred to as *SSL termination*) internally.

When using multiple Awingu nodes for high availability reasons, we recommend to use an external SSL offloader.

In `Certificate Settings`, you can upload or generate SSL certificates. Once the first certificate is added, Awingu will start serving HTTPS on port 443.

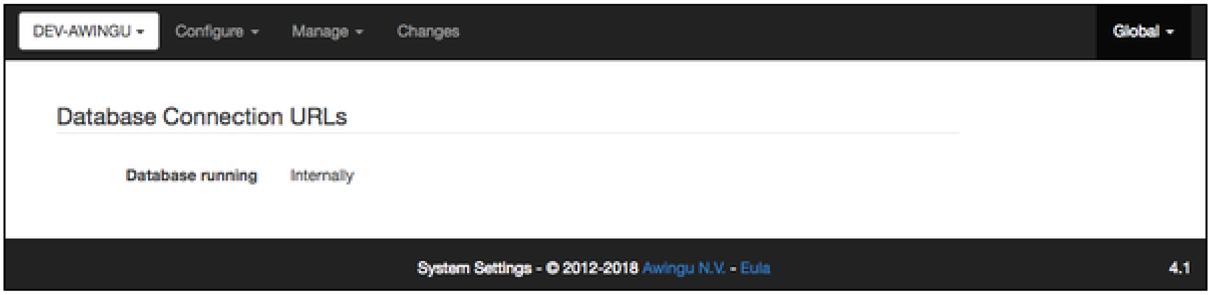
The internal SSL offloader can be used in three states:

- **Optional HTTPS**:
  - If you don't use external SSL offloader, Awingu is accessible via both port 80 (HTTP) and 443 (HTTPS). When accessing via HTTPS, the session cookies have the secure flag enabled: your session cookie is only valid for future HTTPS connections.
  - If you use an external SSL offloader, you will typically not have certificates uploaded in Awingu and the SSL offloader will access Awingu through port 80.
- **Internal SSL offloading with enforced HTTPS**:
  - You are not using an external SSL offloader.
  - Awingu is only accessible via port 443 (HTTPS). All traffic on port 80 (HTTP) will be redirected to 443.
  - The session cookies have the secure flag enabled: your session cookie is only valid for future HTTPS connections.
- **External SSL offloading with enforced HTTPS**:
  - You are using an external SSL offloader.
  - You will typically not have certificates uploaded in Awingu and the SSL offloader will access Awingu through port 80.
  - The session cookies have the secure flag enabled: your session cookie is only valid for future HTTPS connections.

```
Enforced HTTPS with internal or external SSL offloader can only be selected when accessing the System
Settings via HTTPS. This is to avoid that you are locked out of Awingu.
```

Note: if you switch back from HTTPS to HTTP, you will need to clear your browser cache and delete your Awingu cookies to be able to use Awingu again.

Database connection

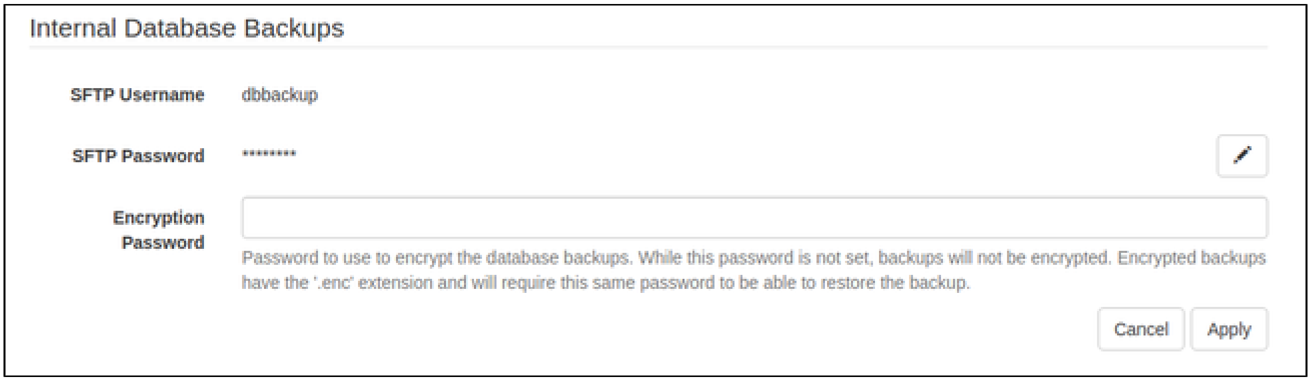


Database Connection URLs

Database running: Internally

Optionally Awingu allows connectivity to an ***external database***. This setting is configured during the installation and cannot be edited afterwards.

Internal Database Backups



Internal Database Backups

SFTP Username: dbbackup

SFTP Password: ********

Encryption Password:

Password to use to encrypt the database backups. While this password is not set, backups will not be encrypted. Encrypted backups have the '.enc' extension and will require this same password to be able to restore the backup.

This parameter is only relevant when the Awingu internal database is used. Awingu creates a backup of the internal database every day and store it on the appliance. You can retrieve this backup and save it on another system via SFTP. The backups are retained on local disk for a period of 3 days, before being discarded. More information: Backup and recovery of the Awingu Database.

You can choose the credentials of the SFTP user that can access the database dump:

- **Username**: SFTP username *dbbackup*. This cannot be changed.
- **Password**: SFTP password.
- **Encryption Password**: Password to use to encrypt the database backups. When this password is not set, backups will not be encrypted. Encrypted backups have the '.enc' extension and will require this same password to be able to restore the backup.

Vault

The vault is needed when you want to enable Single Sign-On in Awingu.

Since the private key for the Awingu Sub-CA allows Awingu to impersonate Windows users, this key is highly sensitive and is stored in a vault inside of Awingu. The vault itself is also encrypted and the encryption key for the vault can either be stored on the Awingu appliance itself (Internally) or on an external Vault provider like Google Cloud Key Management Service or Azure Key Vault.

For more details see Enabling Single Sign-On (SSO)

General Information

License

This section allows you to upload your Awingu license key and displays key information regarding your license. If a license key is in use, and you upload a new key, the previous key gets overwritten. There is only one active key at any point in time.

> The Management User can always sign-in to Awingu, even when the user limit or the expiration date has been reached.

Management User

The management user can log into the System Settings even when Awingu's connectivity to the authentication service has not yet been established. For more information, please refer to the appropriate section of the Awingu installer.

- **Username**: Username of the management user (**cannot** be edited).
- **Whitelisted Subnets**: If enabled, you can only login with the management user from the provided list of subnets. A typical use case is to only allow access from within the company or the data center.

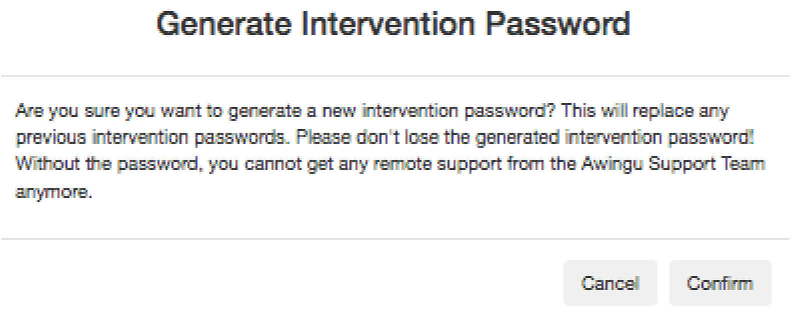
In order to change the password of the management user:

- Login with the username and password of that management user. When OTP or Radius is enabled, you don't need to provide any token.
- In the bottom left, click on the profile menu and select **Account settings**.
- Click on **Change password**.

Remote Support

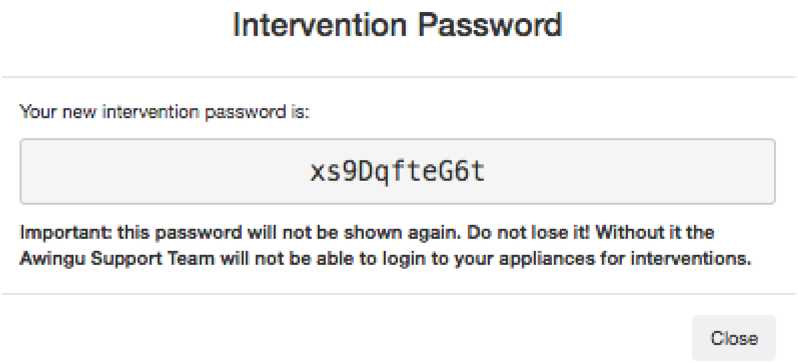
Some interventions by the Awingu Support Team require SSH access. When temporarily opening the SSH port (TCP:22) on your firewall for the intervention, it is recommended to use an intervention password that you can communicate to the Support Team as an additional layer of security. If you don't enable this feature, the Support Team will be able to access your environment without an intervention password.

When you enable the **Intervention Password** a password will generated for you.



Generate Intervention Password

Are you sure you want to generate a new intervention password? This will replace any previous intervention passwords. Please don't lose the generated intervention password! Without the password, you cannot get any remote support from the Awingu Support Team anymore.



Intervention Password

Your new intervention password is:

xs9DqfteG6t

Important: this password will not be shown again. Do not lose it! Without it the Awingu Support Team will not be able to login to your appliances for interventions.

At any point in time you can regenerate the intervention password.

Anonymous Usage Reporting

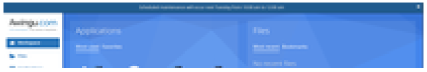
When enabled, the appliance will periodically send anonymised usage data to Awingu. The data does not include any identifiable references, such as names of users, groups, applications etc.

This feature requires your Awingu appliance to have access to https://analytics.awingu.com and can be enabled or disabled at any point in time.

System Message

This feature allows an administrator to send a message to all users of the Awingu environment.

- This message will appear maximum 5 min after the message is set and will be shown at the top of their page (see screenshot below). The user can close the message but it will re-appear again after login.
- The message supports HTML which can be useful if you want to add a link with more information.



Upgrade Version

When a new version of Awingu is published, this version will be shown in the drop-down list.

To reduce the amount of time spent upgrading Awingu, it is possible to download the packages for a version beforehand. You cannot upgrade to any version or download other versions while this is happening.

When clicking Upgrade, the minimum hardware requirements will be validated. See Sizing & Scaling Requirements for more information.

Migrate Audit Logs

> This section is only available on environments that upgraded to Awingu 5.0 and did no yet migrate their logs to the database.

Starting from Awingu 5.0 audit logs are also stored in the database. This section allows you to migrate your existing audit logs to the database. **This will be required to upgrade to Awingu 5.1**

To start the migration process, click on the ‘*Start Migration*’ button.

We strongly advise taking a snapshot prior to performing this operation.

Partner

Enter the contact details of the ***partner*** which is responsible for installation and upgrades of the Awingu platform.

- **Name**: Name of the partner.
- **Address line 1**: Address of the partner.
- **Address line 2**: Address of the partner. (*optional*)
- **Zip or Postal code**: Zip code.
- **City**: City.
- **Location:** state/province/region.
- **Country**: Country.
- **Phone**: Phone number of the partner. (*optional*)

Account Manager

Enter the contact details of the ***account manager***, the prime contact person at your ***partner***.

- **Name**: Name of your contact person.
- **Phone Number**: Phone number of contact person. (*optional*)

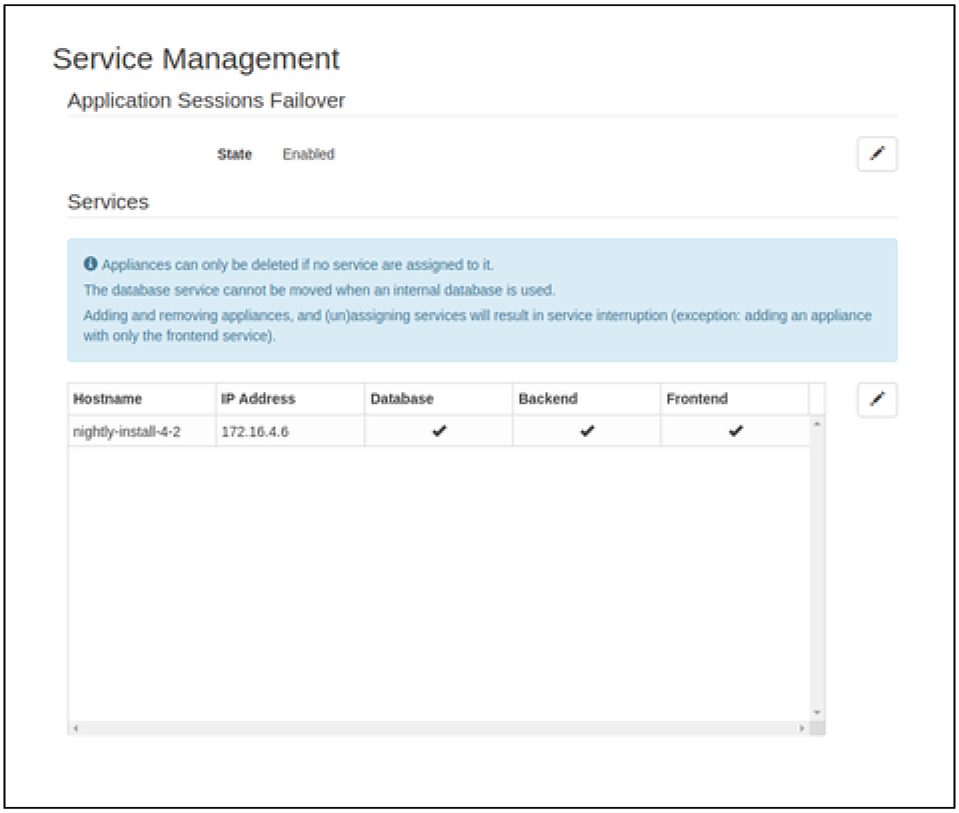
Service Management Settings

Introduction

Service Management enables you to add and remove Awingu appliances (nodes) to your environment, define the roles of each Awingu appliance and configure Application Sessions Failover.
The main page gives you an overview of all registered Awingu appliances and which roles are assigned to them.

Please refer to Sizing & Scaling Requirements for supported multi node architectures.

> ⚠ **Remarks**
> Once an appliance has been added and configured, **you cannot change its IP address**. Doing so will will result in services failing.
>
> To be able to change IP addresses in a multi-node setup, the Awingu environments firsts needs to be scaled down to a single-node.
>
> (1) Multi-node (2) Remove all other nodes (3) Change IP of the single-node (4) Add new nodes (old nodes can be deleted)



Service Management

Application Sessions Failover

State Enabled

Services

ℹ Appliances can only be deleted if no service are assigned to it.
The database service cannot be moved when an internal database is used.
Adding and removing appliances, and (un)assigning services will result in service interruption (exception: adding an appliance with only the frontend service).

Hostname	IP Address	Database	Backend	Frontend
nightly-install-4-2	172.16.4.6	✓	✓	✓

Application Sessions Failover

This feature determines the behaviour when an Awingu node would fail.

- If enabled, Awingu will redistribute all existing application sessions that are actively connected to a user of the failing node to the other available Awingu nodes. Users will not lose their application session and can continue to work after a few seconds.
- If disabled, all existing application sessions on that failing node will be lost. Users will need to restart their applications.

Services

Selecting an appliance from the list, will show its details below the list.

You can modify your environment by clicking the edit button.

Adding Awingu appliances

1. Make sure all TCP, UPD and ICMP network traffic is allowed between all Awingu appliances. The appliances should have the same version as the existing Awingu environment.
2. Click on the pencil next to the table.
3. Click on **Add appliance.**
4. After maximum 10 seconds, the **Discovered Appliances** section will show a list with all Awingu appliances in the network. Discovery of appliances only works when broadcast is allowed on the network. This is usually not the case on public clouds.
5. When using discovery: click on a discovered appliance, change its hostname if desired and click on **Add**.
   When not using discovery: fill-in a hostname and an IP address in the form at the bottom and click on **Add**.
6. Check the roles you want to assign to the new appliance (see further).
7. Repeat steps 3-6 for all appliances.
8. Click on **Update**.

Removing an Awingu appliance

In order to remove an Awingu appliance:

1. Click on the pencil next to the table.
2. Uncheck all roles that were assigned to the appliance.
3. Delete the appliance from the list.
4. Click on **Update.**

> ⊗ If the appliance was still running, Awingu will try to shut it down. **Do not start that appliance again!**

Assigning roles

To assign a role to an Awingu appliance, make sure the corresponding role is ticked for the appliance.

Click **Update** to apply the configuration changes.

In case the update fails due to e.g. system inconsistencies, you can check the option **Ignore operational errors** to continue despite these warnings.
Please consider that this might break your environment! It is recommended to contact support@awingu.com.

Following roles are defined:

- **Database**: Provides the database service to store all metadata. This role cannot be moved. This role is not present when using an external database.
- **Backend**: Provides all services required for internal operation of the Awingu platform (indexer, metering, mq). One appliance with a backend role is enough to serve thousands of concurrent users. For high availability (HA), 3 appliances are required.
- **Frontend**: Provides all APIs and brokering services (frontend, memcache, proxy, rdpgw, worker). This role scales horizontally and is CPU bound.

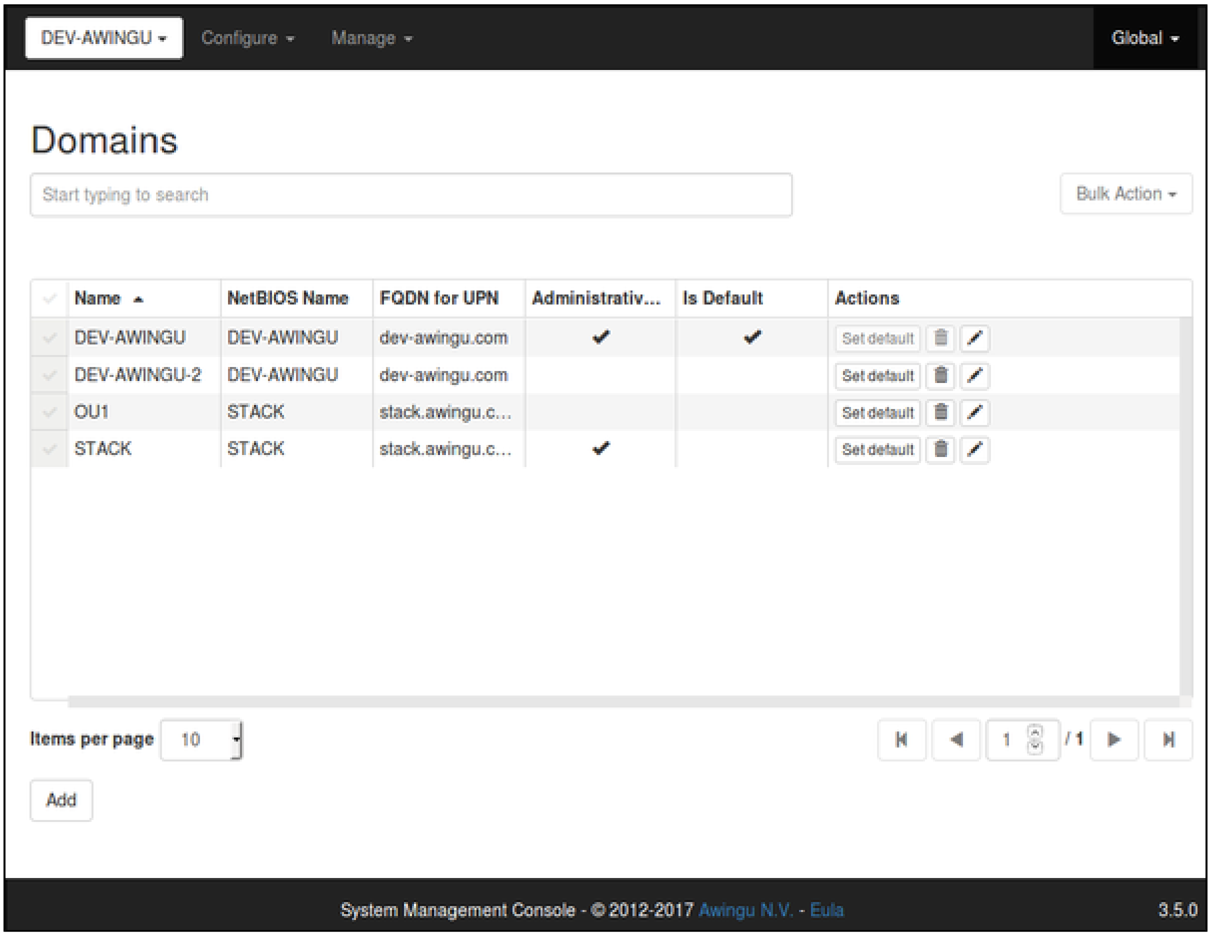
> ⚠ Always make sure that the **backend** role is assigned to 1 appliance (non-HA) or 3 appliances (HA).

Domain Settings

Introduction

Awingu does not store user credentials but instead authenticates and authorizes users based on information retrieved from the existing enterprise authentication and authorization infrastructure. This approach avoids that user credentials need to be maintained over several systems and allows to keep user data in a central location. It also speeds up the roll-out of Awingu as there is no need to configure users onto the Awingu platform.

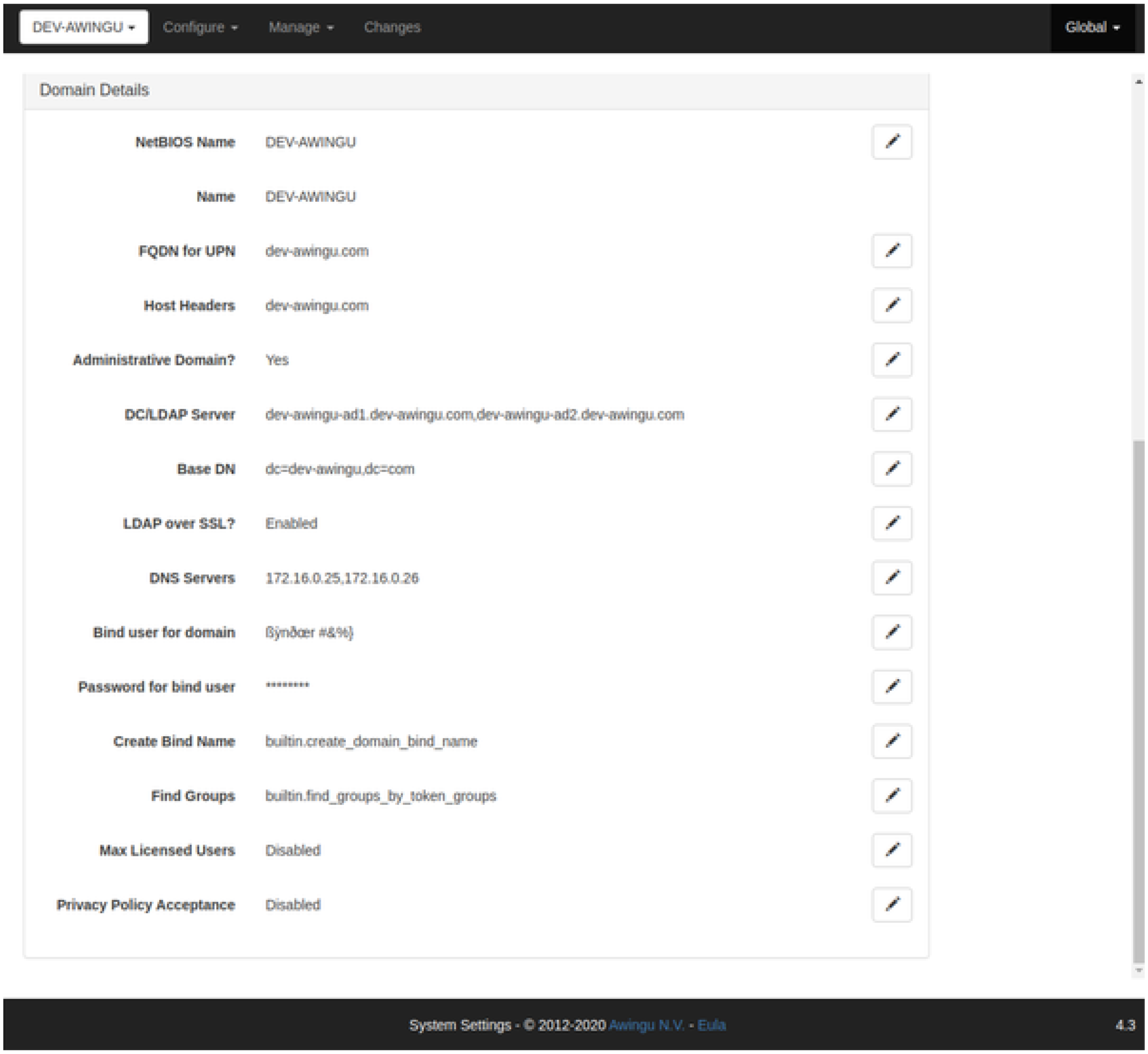
Domains



Domains

Name	NetBIOS Name	FQDN for UPN	Administrativ...	Is Default	Actions
DEV-AWINGU	DEV-AWINGU	dev-awingu.com	✔	✔	Set default
DEV-AWINGU-2	DEV-AWINGU	dev-awingu.com			Set default
OU1	STACK	stack.awingu.c...			Set default
STACK	STACK	stack.awingu.c...	✔		Set default

System Management Console - © 2012-2017 Awingu N.V. - Eula 3.5.0



Domain Details

NetBIOS Name	DEV-AWINGU
Name	DEV-AWINGU
FQDN for UPN	dev-awingu.com
Host Headers	dev-awingu.com
Administrative Domain?	Yes
DC/LDAP Server	dev-awingu-ad1.dev-awingu.com,dev-awingu-ad2.dev-awingu.com
Base DN	dc=dev-awingu,dc=com
LDAP over SSL?	Enabled
DNS Servers	172.16.0.25,172.16.0.26
Bind user for domain	ßÿnðœr #&%}
Password for bind user	********
Create Bind Name	builtin.create_domain_bind_name
Find Groups	builtin.find_groups_by_token_groups
Max Licensed Users	Disabled
Privacy Policy Acceptance	Disabled

Domains can be added using the 'Add' button, or modified by clicking the pencil button in the 'Actions' column of the selected domain.

A *domain* is defined by following properties:

- **NetBIOS Domain Name**: NETBIOS domain name (e.g. MYCOMPANY)
- **Name:** Domain name used in Awingu. Multiple names can refer to the same NetBIOS name.
- **FQDN for UPN**: The FQDN of the domain. E.g. domain.internal
- **Host Headers:** In case of having multiple domains, when reaching Awingu via one of the host headers defined here, the branding of this domain will be used and the domain does not need to be filled-in (the extra field for domain will be hidden at the login page). Multiple host headers can be entered comma separated.
- **Administrative Domain:** When set to yes, admin users of this domain are allowed to configure all domains, global settings and have access to the Dashboard. Admin users can be defined in User Connector Configuration.
- **DC/LDAP server**: FQDN or IP address of the Domain Controller or LDAP Server. E.g. ad01.domain.internal. Multiple servers can be entered comma separated. The first server will always be tried as first one during login.
- **Base DN**: When a user signs in, this base distinguished name (DN) is used to bind via LDAP to the Domain Controller/LDAP server. This can be used to filter access based on organizational unit (OU).
  Example without OU restriction: dc=domian,dc=internal
  Example with OU restriction: ou=Employees,dc=domian,dc=internal

  > ℹ This field can be used to create different Awingu domains, all pointing the same NetBIOS. Only users of the configured OU will be able to login to that domain.

- **LDAP over SSL?**: Requires SSL certificate on Domain Controller or LDAP Server.

  > ⚠ LDAP over SSL is required to allow users to change their password via Awingu.

> ⚠ Please make sure the SSL certificate installed on the AD/LDAP server for LDAPS is encrypted using **SHA256**. A certificate using SHA512 is NOT supported by Awingu. Therefore, LDAPS login will not work with SHA512.

- **DNS Servers**: This DNS server is used to resolve servers matching the FQDN for UPN. Multiple servers can be entered comma separated. E.g. if FQDN for UPN is domain.internal, then fileserver.domain.internal will be resolved with the mentioned DNS server.
- **Max Licensed Users**: If enabled, you can configure the maximum number of concurrent or named (depending on the license) users that are allowed to be logged in to this domain. When set to 0, no domain users can access the domain anymore.
- **Privacy Policy Acceptance**: When set to enabled, each user will have to accept the Privacy Policy the first time they login. This is needed for GDPR compliancy.

Optionally a service user account can be defined which is required for importing labels (users and groups) and applications servers from Active Directory from within System Settings. To configure this service account, following parameters are required:

- **Bind user for domain**: The username of the service account
- **Password for bind user**: The password required to authenticate the service account

> ⚠ For security reasons, it is recommended to create a new read-only user account with limited rights on the Domain Controller/LDAP Server for this purpose only.
> Note that the "Base DN" is not used during the import, meaning that domain admins will be able to see all users/groups/servers of the whole Windows domain, unless the bind user has been configured on the AD to only allow to list the ones of its OU.

Some advanced functionality:

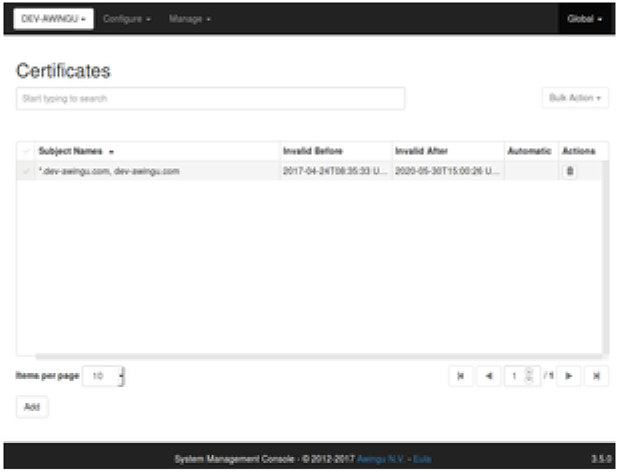
- **Create Bind Name**: defines how to bind user names in LDAP:
    - builtin.create_domain_bind_name (default): bind to LDAP via "DOMAIN\username"
    - builtin.create_username_bind_name: bind to LDAP only via the username
    - builtin.create_uid_bind_name: bind via uid=<username>,ou=Users,<base dn>

  Find Groups: defines how to query the LDAP Server for groups to which a user belongs.
    - builtin.find_groups_by_member_of: find group via memberOf field in LDAP result
    - builtin.find_groups_by_token_groups (default): find group recursively (method 1) Note: this method also fetches the primary group attribute.
    - builtin.find_groups_by_member: find group recursively (method 2)
    - builtin.find_groups_by_uid: find group via UID

Default Domain

A default domain is configured, which will be used if no domain is specified at login time or no correct host header was used.
To change the default domain, use the set default action on the domain to use as default.

Certificate Settings



Certificates

	Subject Names ▾	Invalid Before	Invalid After	Automatic	Actions
✓	*.dev-awingu.com, dev-awingu.com	2017-04-24T08:35:33 U...	2020-05-30T15:00:26 U...		🗑

Introduction

If no external SSL offloader is available, Awingu can handle the SSL offloading (also referred to as SSL termination) internally.

When using multiple Awingu nodes for high availability reasons, we recommend to use an external SSL offloader.

Only when the internal SSL offloader is used, you need to upload or generate the certificates in Awingu via Global > Certificates.

Once the first certificate is uploaded or generated, Awingu will start serving HTTPS on port 443. To enforce HTTPS, please refer to Connectivity Settings.

Generating certificates automatically

If you do not own SSL certificates, you can use the *Automatic* option which will generate and configure SSL certificates provided by the free CA service of https://letsencrypt.org

To generate certificates automatically, click on Add and provide following information:

- **Certificate**: Automatic
- **Subject Names**: the host name(s) you want to create certificates for (e.g. awingu.mycompany.com)

The generated certificates are valid for 90 days. After 60 days, Awingu will renew the certificate. Therefore, the public servers of Let's Encrypt always need to be able to reach the Awingu appliance on port 80 and 443.

> ⚠ Following network requirements are needed in order to request and renew automatic certificates:
>
> - Ports 80 and 443 of Awingu need to be accessible for the **public** servers of Let's Encrypt through all provided subject names.
> - Awingu needs to be able to reach the REST API of Let's Encrypt directly (without the use of an HTTP proxy) through port 443 for *.api.letsencrypt.org.

Please note there is a rate limit of the number certificates per registered domains and the number of duplicate certificates. Those limits are described in the documentation of Let's Encrypt. You can hit this limit easily if you use a subdomain of a service or cloud provider, like *.azure.com. Please use a subdomain you fully control.

Automatic SSL is only available for single node Awingu configuration or for multi node Awingu with only one Frontend service.

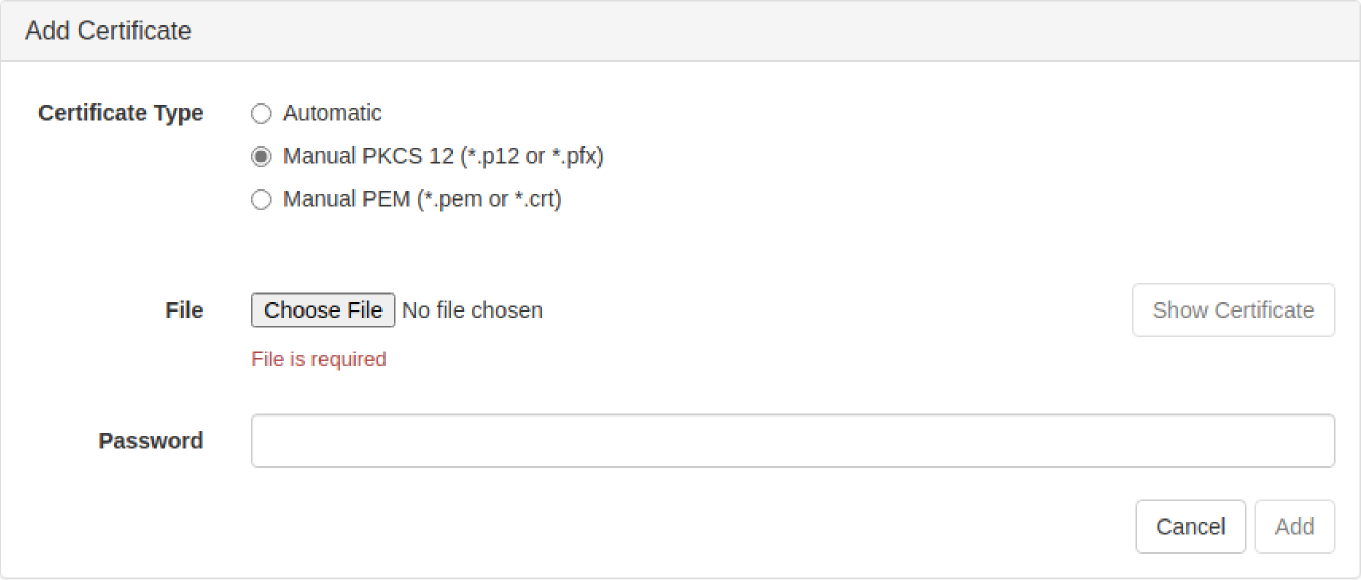
Uploading certificates manually

Awingu supports 2 types of certificates:

- PKCS 12 certificates - typically with `.p12` or `.pfx` extension

- PEM certificates - typically with `.pem` or `.crt` extension

PKCS 12 certificates



Add Certificate

Certificate Type
○ Automatic
● Manual PKCS 12 (*.p12 or *.pfx)
○ Manual PEM (*.pem or *.crt)

File: No file chosen
File is required

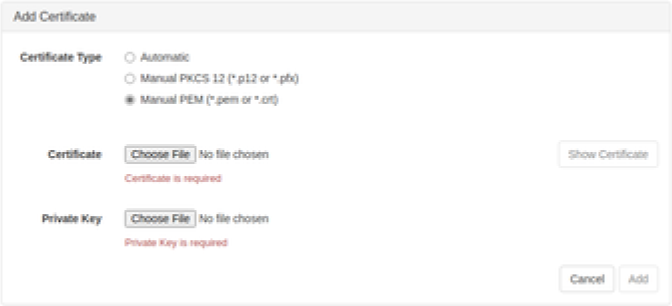
Password

PFX files can contain multiple certificates and can be password protected.

Click on Add and provide the following information:

- **Certificate Type**: Manual PKCS 12
- **File:** The certificate file in `.p12` or `.pfx` format
- **Password (optional):** The password required to decode the certificate

PEM certificates



Add Certificate

Certificate Type
○ Automatic
○ Manual PKCS 12 (*.p12 or *.pfx)
● Manual PEM (*.pem or *.crt)

Certificate: No file chosen
Certificate is required

Private Key: No file chosen
Private Key is required

Click on Add and provide the following information:

- **Certificate Type**: Manual PEM
- **Certificate**: The public certificate file in **.crt format/.pem format**, ASCII file, starting with:

  ```
  -----BEGIN CERTIFICATE-----
  ```

  Make sure the certificate also contains the **intermediate key chain**, otherwise some browsers might not connect to Awingu because the connection is untrusted.
- **Private Key**: The private key file associated with the certificate in **.key format**, ASCII file, starting with:

  ```
  -----BEGIN PRIVATE KEY-----
  ```

or

```
-----BEGIN RSA PRIVATE KEY-----
```

PEM Certificates with passphrases

If you open the certificate key file and see binary characters instead of the BEGIN (RSA) PRIVATE KEY header, this means your certificate key is still encrypted with a passhprase. The Awingu SSL offloader cannot start automatically when the private key is still encrypted using a passphrase. Therefore you'll need to remove the passphrase from the private key first before uploading the key file. You can remove the passphrase by using the openssl command as follows (you will also be prompted to type in your passphrase):

```
openssl rsa -in encrypted.key -out decrypted.key
```

Self-Signed Certificates

Although not recommended Awingu also supports self-signed certificates. Using self-signed certificates will show a security warning when accessing the site but can be created for free. One of the easiest ways to do this is to use http://www.selfsignedcertificate.com/

Certificate content

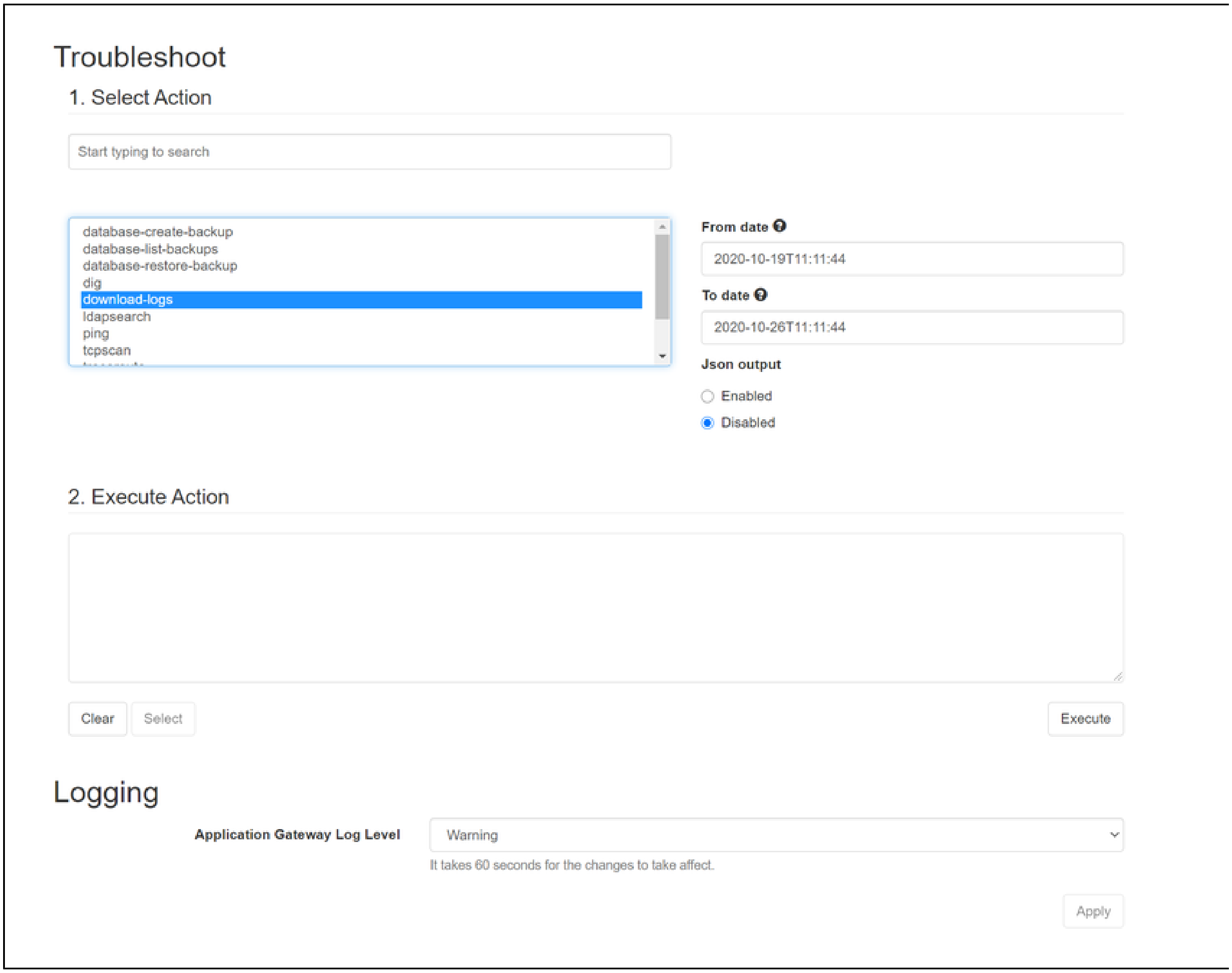
To validate if your certificate is correct - e.g. you want to make sure the certificate contains the intermediate key chain - you can visualize the certificate’s content using the *Show Certificate* button.

Replacing and deleting certificates

When you want to replace a certificate, e.g. because the existing one will expire soon, you first upload the new certificate and then delete the old one.

⚠ Expired manual certificates are not automatically deleted and are still offered to the browsers, which will cause a security warning for the user.

If you are deleting the last certificate of the subject name you are now browsing to, you will need to go manually to HTTP (if HTTPS is not enforced in Connectivity Settings) after deletion. If HTTPS is enforced, you need to go to another subject name you still have a certificate for. You won't be able to delete the last certificate if HTTPS is enforced to avoid that you cannot reach Awingu anymore.



Troubleshoot

1. Select Action

Start typing to search

From date: 2020-10-19T11:11:44

To date: 2020-10-26T11:11:44

Json output
○ Enabled
● Disabled

2. Execute Action

Logging

Application Gateway Log Level: Warning

It takes 60 seconds for the changes to take affect.

The troubleshoot page offers some tools to allow you to manage internal database backups and to troubleshoot why your configuration is not working as expected.
The steps are as follows:

1. Select Action:
   - Select an troubleshoot action to execute
   - Some actions need arguments. Please enter them.
2. Select Target Appliance(s) to execute action on
3. Execute Action:
   - Execute: execute the selected action and the output will be shown in the text box
   - Clear: empty the output text box
   - Select: select all output in the output text box

All actions executed via the Troubleshoot page are logged into the log files. If you enter passwords in the commands, they will be logged in plain text. Please use the data of dummy users for all troubleshooting actions.

Database actions

The database actions allow you to manage backups of the internal Awingu databases.

Following actions are provided:

Action	Description
database-list-backups	Generates a list of all available database backups on the Awingu environment
database-create-backup	Created a new backup of all internal Awingu databases
database-restore-backup	Restores the database backups of the provided file

More information on Backup and recovery of the Awingu Database.

dig

Dig is a DNS lookup utility.

Example of arguments to use:

- Lookup for www.example.com on the DNS server with IP address 8.8.8.8

  ```
  @8.8.8.8 www.example.com
  ```

- Lookup for repo-pub.awingu.com. No DNS server is given, so the one configured in the Connectivity tab is used.

  ```
  repo-pub.awingu.com
  ```

Dig returns the answer from the DNS server (see Answer Section in the output)

More information: dig man page.

download-logs

Download the log files of the Awingu appliance. You can provide following arguments to change the output format and time period:

- *From & To date:* By default all logs from the last 7 days will be fetched. You can specify a from and a to date/time in UTC ISO format as arguments.
- *Json output:* By default the different fields of a log statement are seperated by spaces. By enabling newline-delimited Json output, the fields are available as Json properties and different log statements are separated by newlines.

A link to the log files will be shown in the output field. If the ZIP file is not ready yet, the file name starts with INPROGRESS. Every hour, ZIP files older than 1 hour will be cleaned-up.

ldapsearch

Ldapsearch is a LDAP utility.

Example of arguments to use to simulate the default Awingu behavior when User1 signs in:

```
-LLL -H ldap://domain.example.com:389 -b 'dc=domain,dc=example,dc=com' -D
'DOMAIN\User1' -w 'password' '(&(sAMAccountName=User1)(objectClass=user))'
```

Argument definition:

- -LLL: show the output in LDIF format
- -H <ldap_url>: the URL of the LDAP server. Typically: 389 (no SSL)
- -b '<base_dn>': the starting point for the LDAP search
- -D '<bind_dn>': the distinguished name to bind to the LDAP directory. See Functions in User Connector tab:

    - function builtin.create_domain_bind_name (default): '<domain_name>\<username>'
    - function builtin.create_username_bind_name: '<username>
- -w '<password>': the password for the user to bind with
- '<filter>': LDAP search filter. The filter used by Awingu: '(&(sAMAccountName=<username>)(objectClass=user))'

Ldapsearch returns the LDAP search result. Interesting output lines are the ones starting with "memberOf", to see the list of AD security groups the user belongs to.

More information: ldapsearch man page.

ping

Ping is a ICMP echo request sending tool.

Example of arguments to use:

- Ping 3 times to example.com:

```
-c 3 example.com
```

- Ping 5 times to example.com and only show IP addresses (n = numeric):

```
-c 5 -n example.com
```

More information: ping man page.

tcpscan

Scans for open TCP ports. This action requires following arguments:

- Host: hostname or IP address
- Port: single port, port range (e.g. 80-100) or comma separated list of ports (e.g. 80,443).

traceroute

Traceroute is a tool print the route packets trace to network host

Example of arguments to use:

- Trace route to example.com

```
example.com
```

- Trace route to example.com and only show IP addresses (n = numeric):

```
-n example.com
```

More information: traceroute man page.

udpscan

Scans for open UDP ports. This action requires following arguments:

- Host: hostname or IP address
- Port: single port, port range (e.g. 80-100) or comma separated list of ports (e.g. 80,443).

uptime

Uptime is a utility that tells how long the system has been running.

It shows some additional information, example:

```
 15:21:06 up 2 days, 1:46, 0 users, load average: 0.19, 0.25, 0.25
```

- 15:21:06: current time of the Awingu VM in UTC. If the time is not correct, this can indicate a faulty NTP server.
- up 2 days, 1:46: number of days and hours since the last time the Awingu VM has booted-up.
- 0 users: number of system users logged-in to the system. Is typically 0.
- load average: system load of past 1, 5 and 15 minutes. The Awingu VM is overloaded if the value is higher than the number of CPUs.

More information: uptime man page.

Logging

In this section, the log level of the Application Gateway can be modified. This can be very helpfull when troubleshooting an issue with applications. Changing the log level does not have service impact.

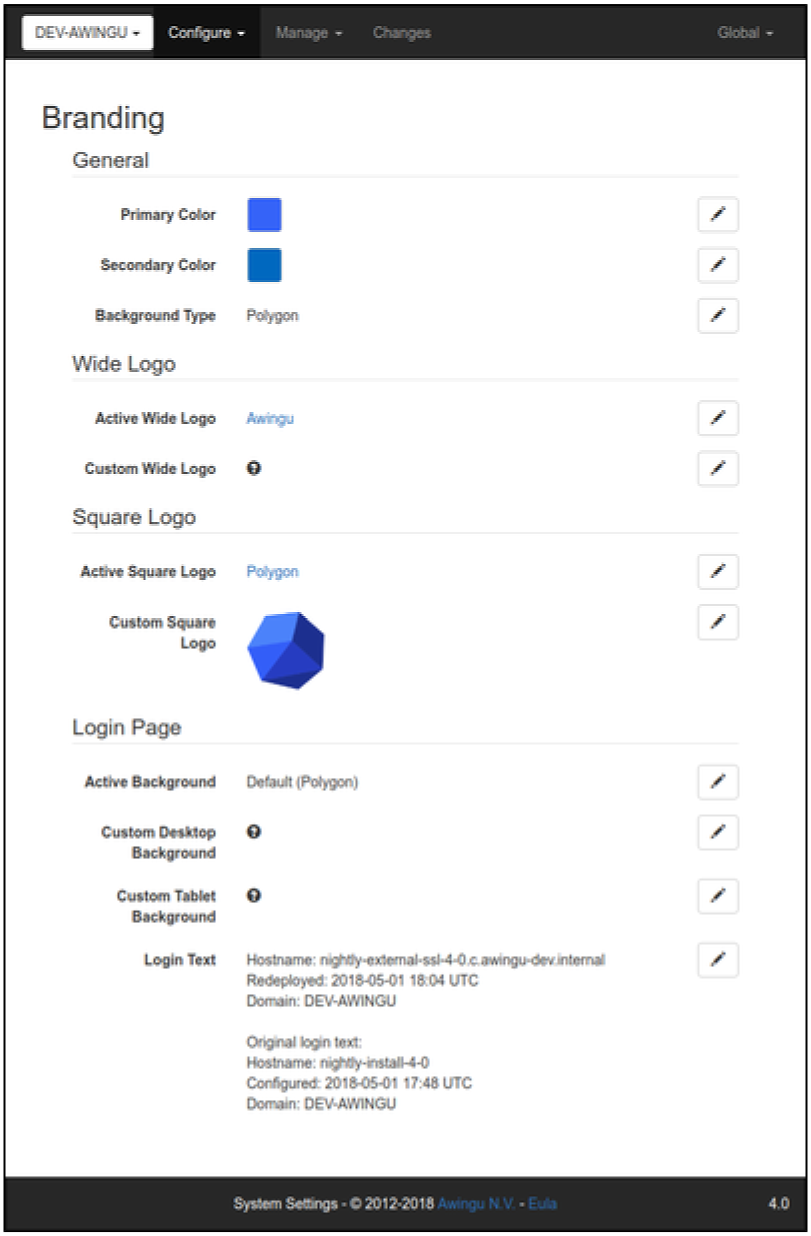
Be aware however that if you change the log level to Info, Debug or Trace a lot more logs will be generated. As there is a maximum of 8GB disk space allocated for logs, it will not have impact on the overall appliance but logs of other services will get cleaned up sooner.

System Settings - Configure

Domain specific settings are configured here:

- Branding Configuration
- Feature Configuration
- User Connector Configuration

Branding Configuration



Branding

General

Primary Color 🟦

Secondary Color 🟦

Background Type Polygon

Wide Logo

Active Wide Logo Awingu

Custom Wide Logo

Square Logo

Active Square Logo Polygon

Custom Square Logo

Login Page

Active Background Default (Polygon)

Custom Desktop Background

Custom Tablet Background

Login Text Hostname: nightly-external-ssl-4-0.c.awingu-dev.internal
Redeployed: 2018-05-01 18:04 UTC
Domain: DEV-AWINGU

Original login text:
Hostname: nightly-install-4-0
Configured: 2018-05-01 17:48 UTC
Domain: DEV-AWINGU

System Settings - © 2012-2018 Awingu N.V. - Eula 4.0

Multi-domain branding behavior

Each domain has its own branding configuration:

- When you access the login page via the host header defined in Domain Settings:
    - The branding of that domain is shown.
    - The *Domain* field on the login page is hidden.
- When you access the login page via a non-defined host header and there is only 1 domain configured:
    - The branding of that only domain is shown.
    - The *Domain* field on the login page is hidden.
- When you access the login page via a non-defined host header and there are multiple domains configured:
    - The branding of the Default Domain is shown.
    - The *Domain* field is shown on the login page.

- When you are logged in:
    - The branding of the applicable domain is shown.

Configuration options

For each domain following settings can be shown:

General

- **Primary Color:** The base color used to generate the background, polygon, pop-ups and favicon of the Awingu frontend for this domain. It is recommend to choose a bright color.
- **Secondary Color:** The color used in the Awingu frontend for buttons, folder icons, etc.
- **Background Type:** Whether to have the Awingu polygon background or a plain color. In both cases the primary color is used. Note that the background of the login page can be customized further on this page.

Wide Logo

- **Active Wide Logo**: choose between the default Awingu logo and your own custom logo. The logo is shown on the top left of the Awingu frontend on the login page and the non-collapsed sidebar.
- **Custom Wide Logo**: upload an image for your custom logo:
    - Maximum file size: 100 KiB
    - Logo area: 159 x 70 px (when you scroll down, the logo area reduces to 159 x 30 px)

Square logo

- **Active Square Logo**: choose between default Awingu polygon (with the color based on the primary color) and your own custom square logo. The logo is shown as favicon and on the collapsed sidebar.
- **Custom Square Logo**: PNG, JPG, SVG or ICO file of max. 2 MiB. Image needs to be square. Best results with PNG of 512 x 512 px or SVG image.

Note that if you have already accessed Awingu via the same browser before changing the square logo, you might need to clear your browser cache to see the favicon being changed.

Login Page

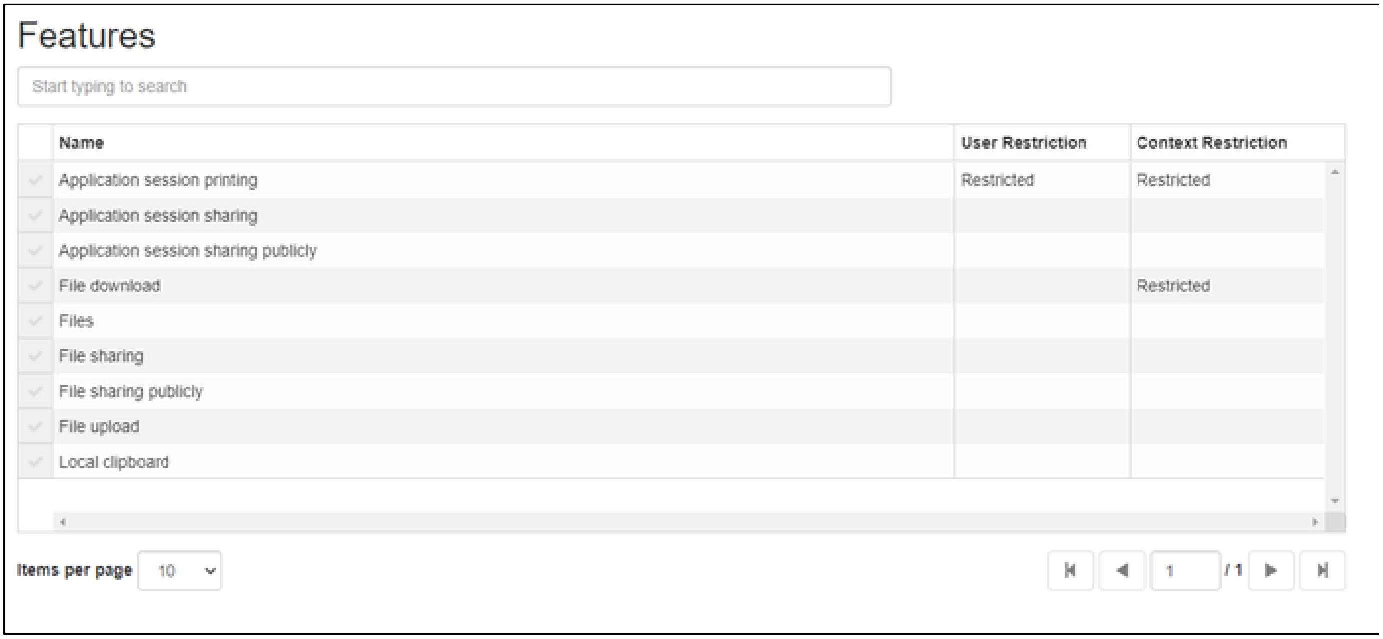
- **Active Background**: choose between the default Awingu background image and your own custom background on the sign-in page.
- **Custom Desktop Background**: upload an image for your custom background for desktops (= screen width or height is more than 1280 pixels)
    - Maximum file size: 500 KiB
    - Recommended resolution: 3000x2100.
- **Custom Tablet Background**: upload an image for your custom background for tablets (= screen width or height is less than 1280 pixels)
    - Maximum file size: 150 KiB
    - Recommended resolution: 1280x860.
- **Login Text**: A free-field text, beneath the login credentials area, to put company specific information such as e.g. legal disclaimers. HTML tags are allowed.

Note about the background images:

- Rescaling (both scale-up and scale-down) is done while keeping the aspect ratio.
- When the scaled image is smaller than the canvas height, the upper and lower part will be cut-off equally.
- When the scaled image is smaller than the canvas width, the left and right part will be cut-off equally.
- The white banner with the logo will cover the upper part of the background image.

Feature Configuration

- Behavior
- Application session printing
- Application session sharing (publicly)
- File download
- Files
- File sharing (publicly)
- File upload
- Local clipboard



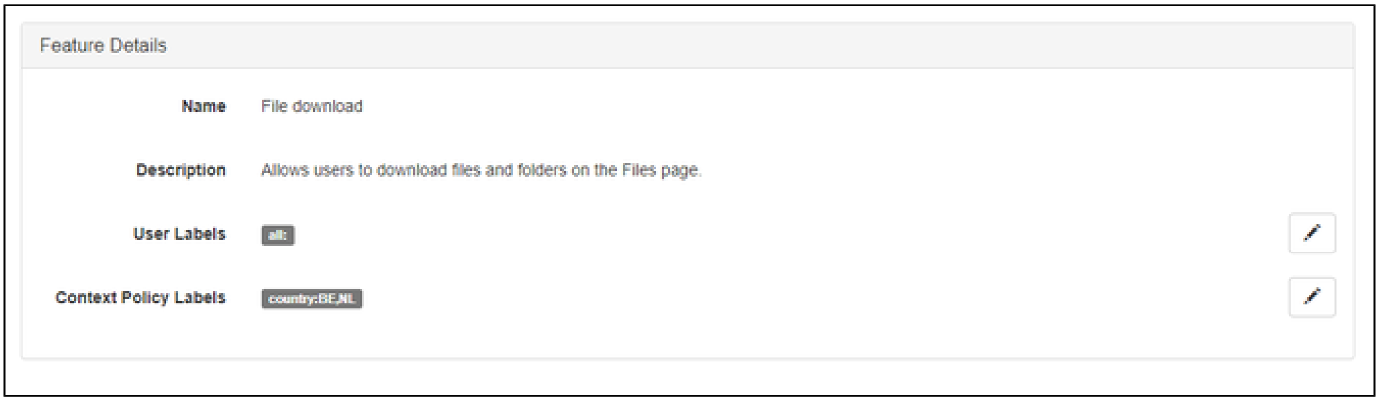
Features

Start typing to search

	Name	User Restriction	Context Restriction
✓	Application session printing	Restricted	Restricted
✓	Application session sharing		
✓	Application session sharing publicly		
✓	File download		Restricted
✓	Files		
✓	File sharing		
✓	File sharing publicly		
✓	File upload		
✓	Local clipboard		

Items per page 10

1 / 1



Feature Details

Name File download

Description Allows users to download files and folders on the Files page.

User Labels all:

Context Policy Labels country:BE,NL

Behavior

All features listed are enabled for users depending on their User Labels and Context Policy Labels.

When the label of a user matches one the User Labels configured for a feature, the security context of the user will be validated against the Context Policy of that feature.

- To enable a feature for all users of the domain, please attach the predefined *all:* User Label to that feature and leave the Context Policy Labels field empty.
- To disable a feature for all users of the domain, please remove any User Labels from that feature.

To create custom labels and to find more information, please refer to Label Management.

Application session printing

When disabled, printing using the 'Virtual printer' within streamed application will not be possible. Printing using other printers configured on application servers will still be possible.

Application session sharing (publicly)

Defines if application session sharing is disabled all together or only disabled for public access. A list of possible scenarios:

The user does not belong to either *Application session sharing* and *Application session sharing publicly* user labels:

- The feature to share application sessions with other users is disabled.
- The Share session polygon button is not shown.

The user only belongs to *Application session sharing* users labels and his security context is valid:

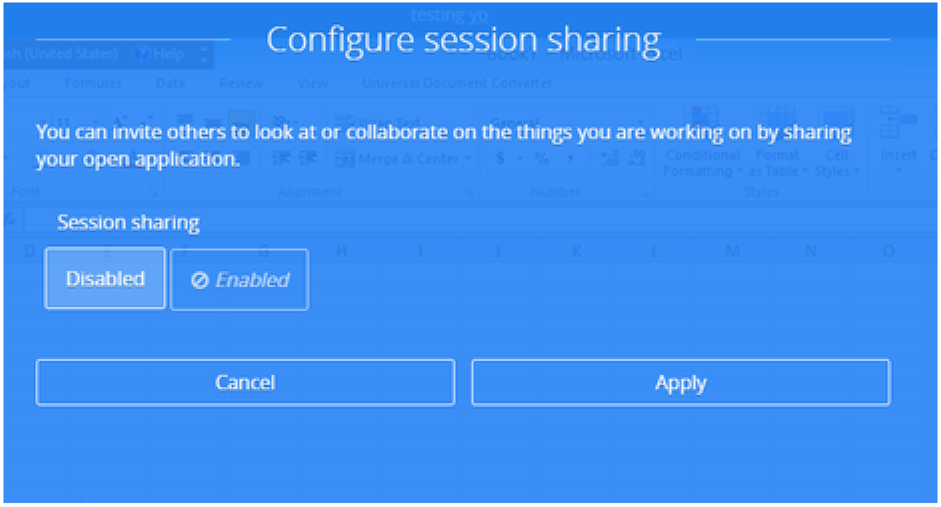
- He can only share his application sessions with users from the same Awingu Domain.

The user belongs to *Application session sharing publicly* user labels and his security context is valid:

- He can share his application session with anyone as long as they have the share link.
- Note: it does not matter if he also belongs to the *Application session sharing* user labels.

The user belongs to *Application session sharing publicly* user labels and his security context is invalid:

- The button to enable session sharing will indicate that due to an invalid security context, session sharing is not allowed.



Configure session sharing

You can invite others to look at or collaborate on the things you are working on by sharing your open application.

Session sharing: Disabled

- Note: it does not matter if he also belongs to the *Application session sharing* user labels.

Note: This feature is accessible in a streamed app when clicking on the polygon and then on the share button.

File download

When disabled, the *Download* action is disabled for all files and folders on the Files page.

Files

When disabled, the *Folders* section on the Files page is removed. If File sharing is disabled, too, the complete Files page is removed.

File sharing (publicly)

Defines if file sharing is disabled all together or only disabled for public access. A list of possible scenarios:

The user does not belong to either *File sharing* and *File sharing publicly* user labels:

- The *Shares* section on the Files page is removed. If Files is disabled, too, the complete Files page is removed.
- The *Share* action is disabled for all files and folders.

The user only belongs to *File sharing* users labels and his security context is valid:

- He can only create file shares that can be accessed by someone from the same Awingu Domain.
- He will be able to choose Users where he can add specific users and groups or choose Domain so everyone from the Awingu Domain can access the file.

The user belongs to *File sharing publicly* user labels and his security context is valid:

- He can create files shares that can be accessed by anyone as long as they have the share link.
- Note: it does not matter if he also belongs to the *File sharing* user labels.

The user belongs to *File sharing publicly* user labels and his security context is invalid:

- The *Share* action will indicate that due to an invalid security context file sharing is not allowed.
- Note: it does not matter if he also belongs to the *File sharing* user labels.

File upload

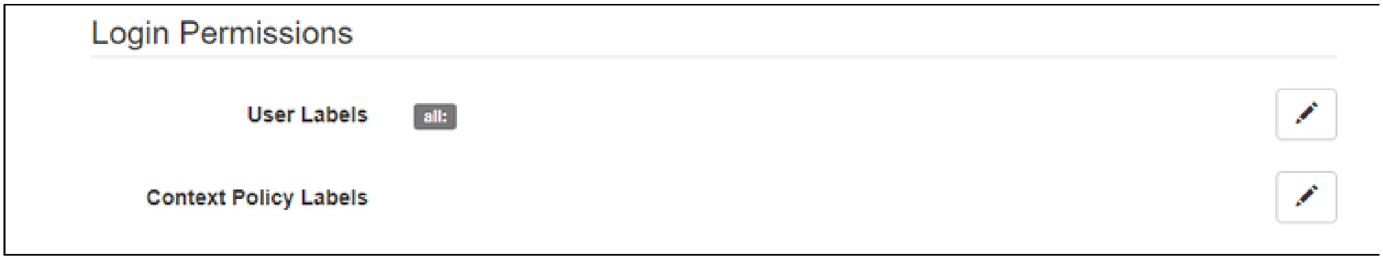
When disabled, the *Upload* action is disabled for all files and folders on the Files page.

Local clipboard

When disabled, using you cannot copy/paste data from streamed applications to your local device and vice versa.

User Connector Configuration

Login Permissions



Login Permissions

User Labels: all:

Context Policy Labels

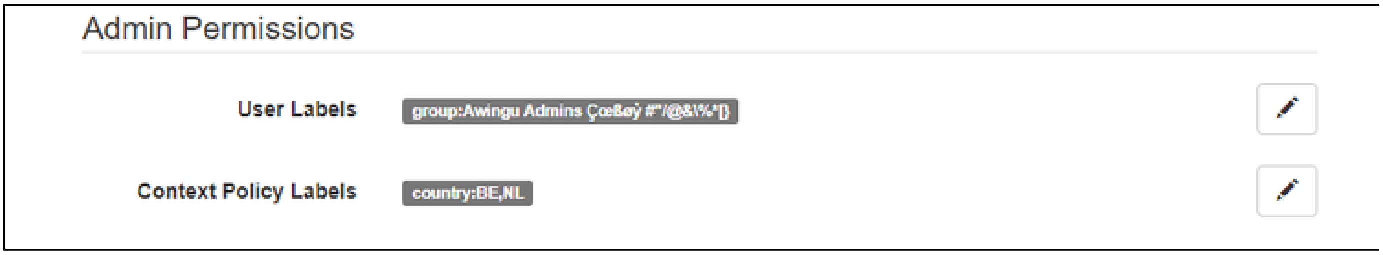
In this section, you define which users are allowed to login by using the label system.

- **User Labels:** Users with at least one of these labels will be able to log in (if all users can log in, add the "all:" label)
- **Context Policy Labels:** Users will only be able to log in if they have a valid context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application. No labels means there are no restrictions.

See Label Management (User and Context Policy Labels) for a more information and examples.

Enable Multi-Factor Authentication on Login
To enable Multi-Factor Authentication for all users when logging in, the 'mfa:required' context label will need to be added to the Context Policy Labels.

Admin Permissions



Admin Permissions

User Labels: group:Awingu Admins Çœßøÿ #"'@&!%*[]

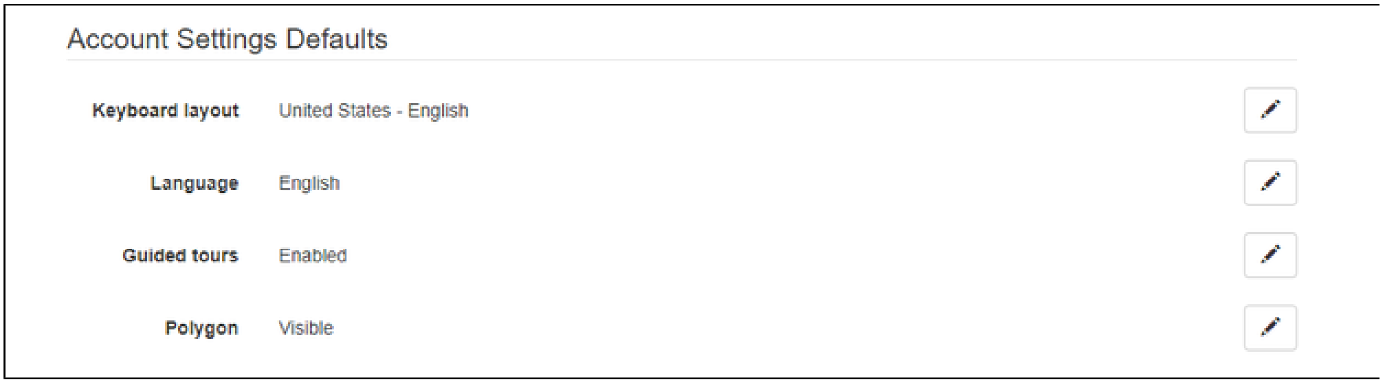
Context Policy Labels: country:BE,NL

In this section, you define which users are Domain Administrators and which security context is required to be a Domain Administrator.

- **User Labels:** Users with at least one of these labels will be Domain Administrators
- **Context Policy Labels:** Users will only receive the Domain Administrator role if their context is valid. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the feature.

See Label Management (User and Context Policy Labels) for a more information and examples.

Account Settings Defaults



Account Settings Defaults

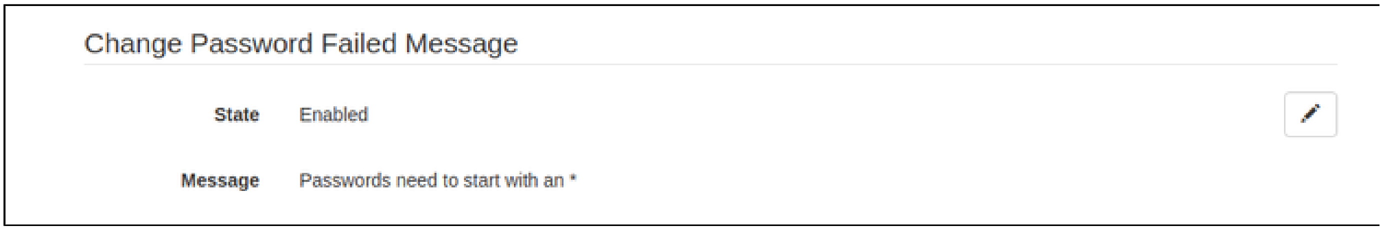
Keyboard layout	United States - English
Language	English
Guided tours	Enabled
Polygon	Visible

This section allows you to define default profile values for users of a domain.

- **Keyboard layout:** the default configured keyboard layout for users of this domain
- **Language:** the Awingu interface's language for users of this domain. By default Awingu will use the browser's default language, if this is unknown to Awingu, it will fall back to this language configured for the domain.
- **Guided tours:** defines if the guided tours are shown for new users of this domain. Note: guided tours will not appear when the browser size is too small.
- **Polygon:** defines if the polygon is shown by default for new users of this domain.

Please note that a user can always update these settings on his/her Account Settings page.

Change Password Failed Message

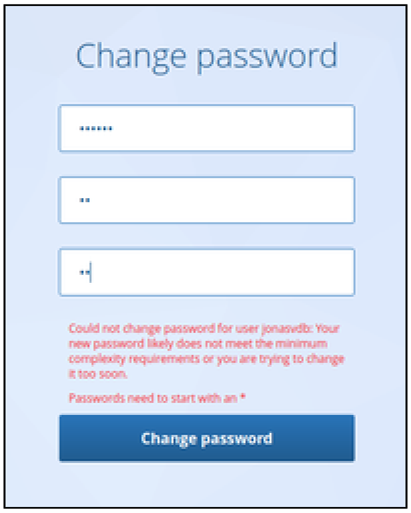


Change Password Failed Message

State	Enabled
Message	Passwords need to start with an *

When a user tries to change his password but it fails due to not meeting the minimum complexity requirements, a custom error message can be added by the administrator.

This message can be used to to inform the users about specific requirements.

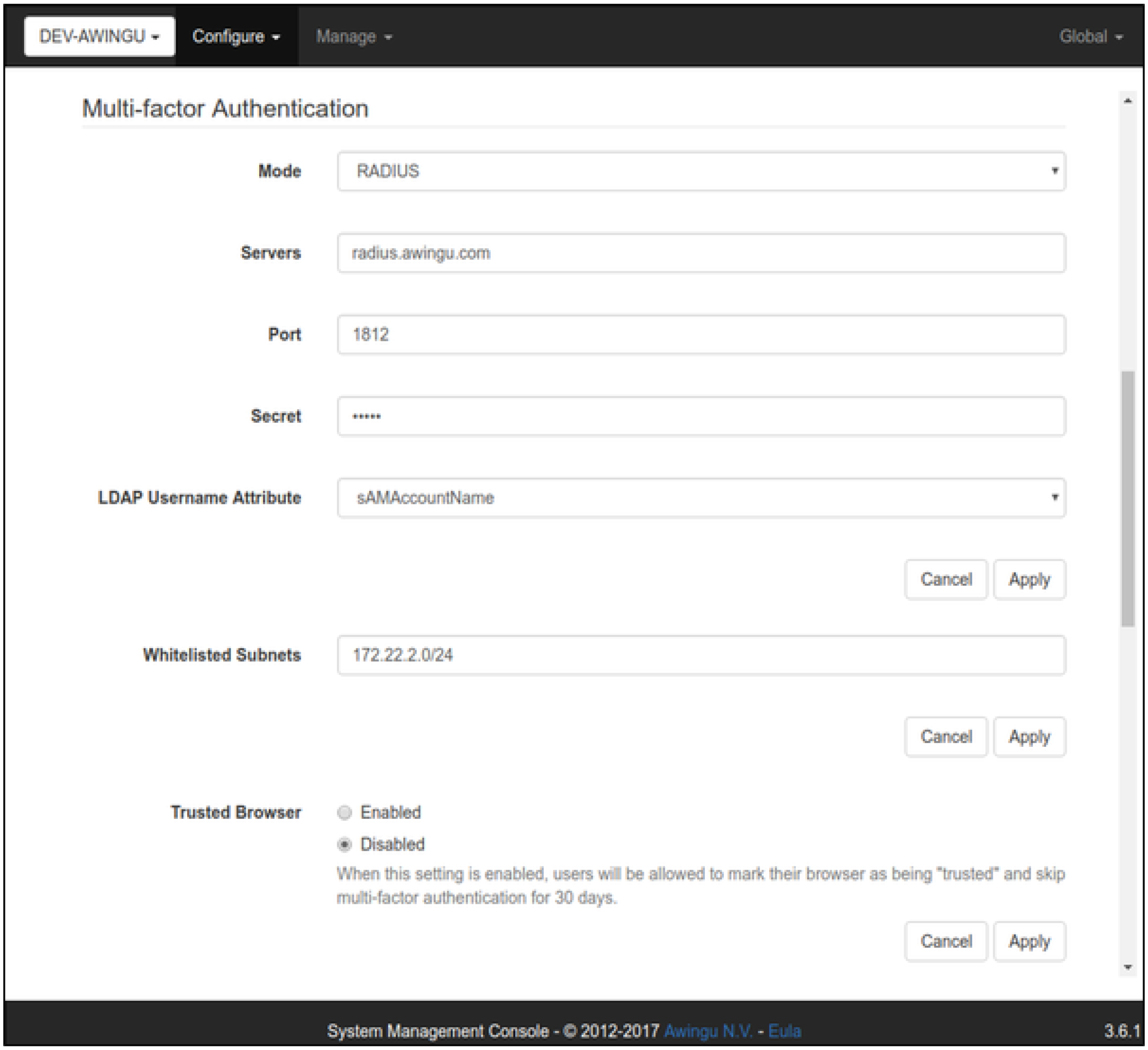


Change password

Could not change password for user jonasvdb: Your new password likely does not meet the minimum complexity requirements or you are trying to change it too soon.

Passwords need to start with an *

Multi-factor Authentication



Multi-factor Authentication

Mode: RADIUS

Servers: radius.awingu.com

Port: 1812

Secret: •••••

LDAP Username Attribute: sAMAccountName

Whitelisted Subnets: 172.22.2.0/24

Trusted Browser: ○ Enabled ● Disabled

When this setting is enabled, users will be allowed to mark their browser as being "trusted" and skip multi-factor authentication for 30 days.

Awingu provides out-of-the-box one-time-password (OTP) support and integrates with a number of Multi-factor Authentication providers.

When enabled, each time a user wants to sign-in to Awingu, not only the LDAP/AD credentials need to be provided, but (s)he will need to generate a token via an app (e.g. Google Authenticator for standard OTP) or a hardware token.

Multi-factor authentication is disabled by default but can be enabled by selecting the desired integration mode.

- **Workspace OTP: Counter Based:** Leverages the built-in counter based one-time-password (OTP) functionality
  - The first time a user wants to sign-in, (s)he needs to download Google Authenticator (iOS/Android) or Auth7 (Windows Phone) - or any other application supporting counter based one-time password generation (e.g. on their smartphone)- and set-up his/her device on via the Awingu sign-in page.
  - **Issuer name:** The company name shown to the user in the OTP application.
  - **Manage User Token Count**: Allows to reset the token count for specific users. When the token is reset, the user will need to set-up his/her device again.
- **Workspace OTP: Time Based**: Leverages the built-in time based one-time-password (OTP) functionality
  - The first time a user wants to sign-in, (s)he needs to download Google Authenticator (iOS/Android) or Microsoft Authenticator -or any other application supporting time based one-time password generation (e.g. on their smartphone)- and set-up his/her device on via the Awingu sign-in page.
  - **Issuer name:** The company name shown to the user in the OTP application.
  - **Manage User Token Count**: Allows to reset the token count for specific users. When the token is reset, the user will need to set-up his/her device again.
- **Duo Security:**
  For more information: Integrating Awingu with DUO
  - **API Hostname:** The Duo Auth API configured hostname
  - **Integration Key:** The Duo Auth API integration key
  - **Secret Key:** The Duo Auth API secret key

- **RADIUS:** The token will be validated using an external RADIUS server (Note: Chap (v2) authentication schema not supported) The RADIUS server needs to be configured to not increase the counter for a failed attempt. For FreeRadius, this means adding no_incremement_hotp to auth requisite in the radiusd config file.
  - **Servers:** Comma separated list of hosts or IP addresses of the RADIUS server
  - **Port:** Port number the RADIUS server is listening on
  - **Secret:** The secret configured in the RADIUS server
- **SMS PASSCODE:** The token will be validated using the SMS PASSCODE RADIUS server
  - **Servers:** Comma separated list of hosts or IP addresses of the SMS PASSCODE RADIUS server
  - **Port:** Port number the SMS PASSCODE RADIUS server is listening on
  - **Secret:** The secret configured in the SMS PASSCODE RADIUS server

For all MFA providers, you can configure following additional setting:

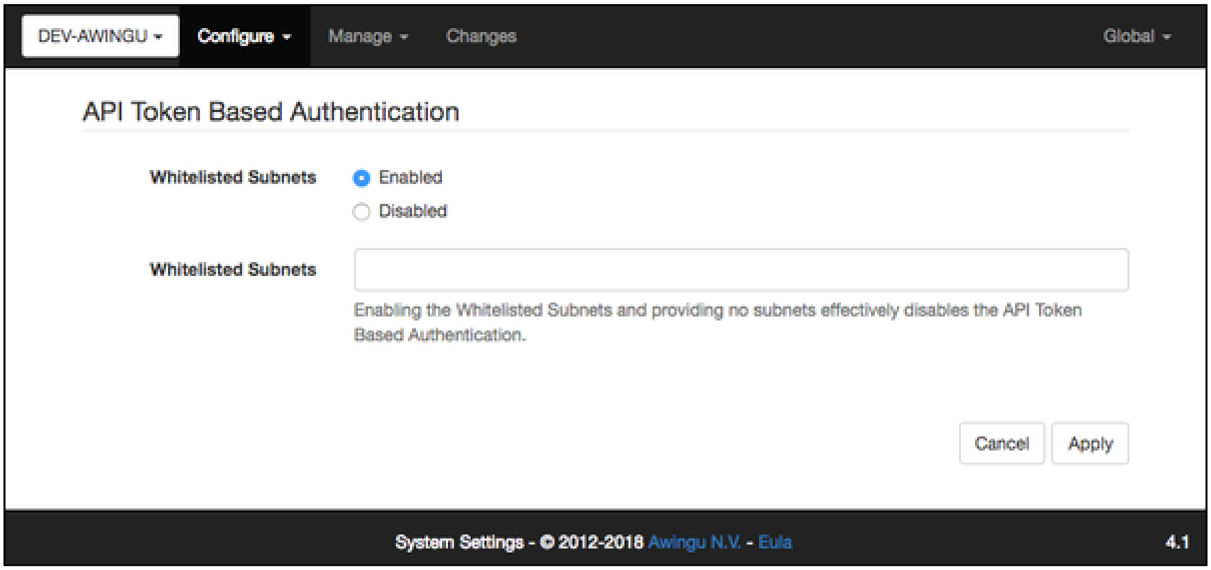
- **LDAP Username Attribute:** the LDAP attribute should be used to provide as username to the provider, via the **LDAP Username Attribute** field. One of following attributes can be chosen:
  - sAMAccountName: corresponds with the login name without UPN on Windows Domain Controller
  - NETBIOS\sAMAccountName: same as sAMAccountname, but with the NetBIOS name prefixed
  - userPrincipalName: corresponds with the UPN on Windows Domain Controller
  - uid: corresponds with the login name without UPN on OpenLDAP
- **Whitelisted subnets:** Comma separated list IPv4 subnets. For users accessing Awingu from these subnets, Multi-factor Authentication will be skipped.

  When using a reverse proxy server in front of Awingu, please make sure you forward the client's originating IP address using the *X-Forwarded-For* header. See SSL offloader, reverse proxy or loadbalancer settings.

- **Whitelisted User Labels:** For users that belong to one of the user labels Multi-factor Authentication will be skipped.
- **Trusted Browser:** If enabled, users will be asked if they trust the device. If so, no MFA will be required for 30 days. Note that if the user deletes her browser cookies, MFA will be required again.

The management user (created during installation) does not need to use any form of MFA to login. To avoid access with that user from the public internet, you can limit subnets from where that user can login on General Information.

API Token Based Authentication



API Token Based Authentication

Whitelisted Subnets ● Enabled ○ Disabled

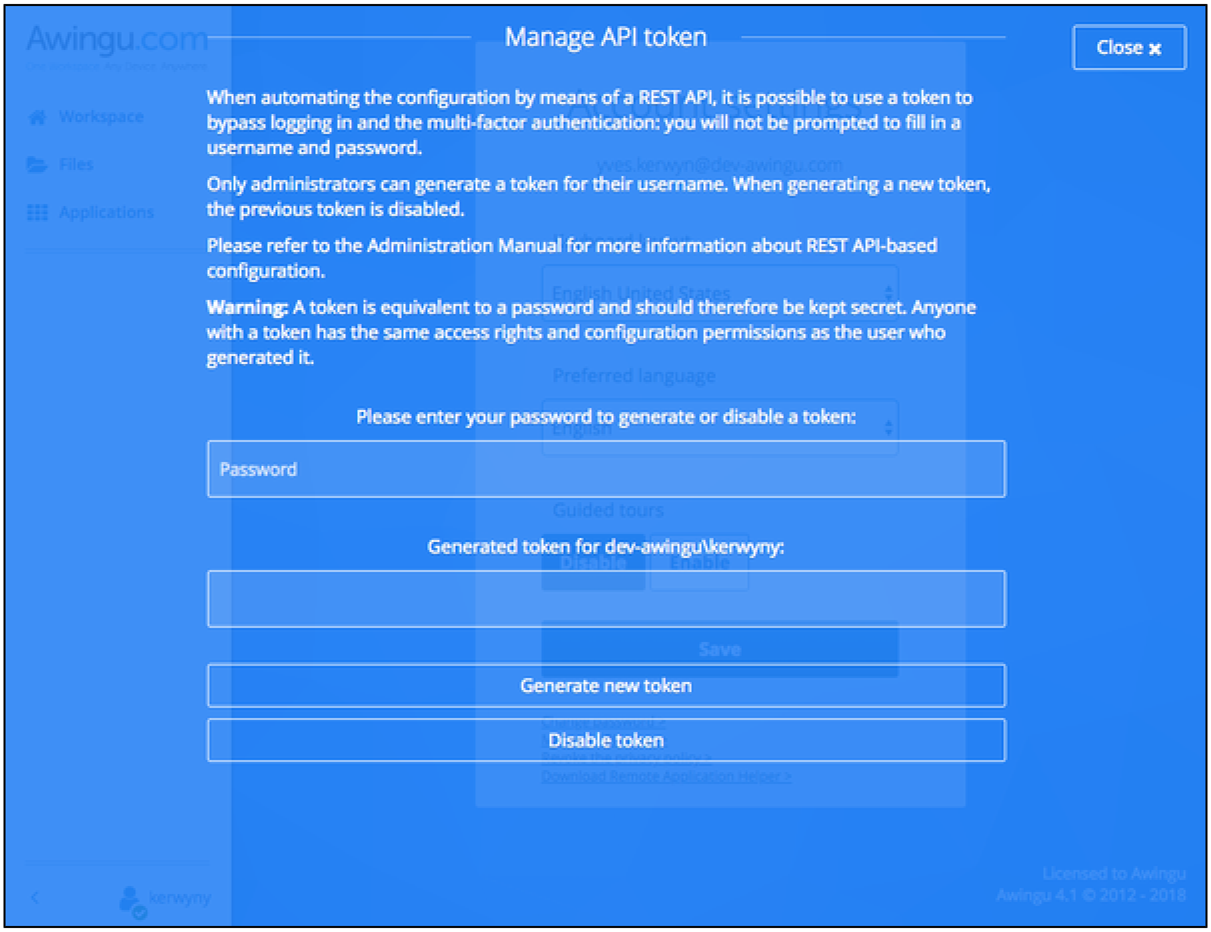
Whitelisted Subnets

Enabling the Whitelisted Subnets and providing no subnets effectively disables the API Token Based Authentication.

Next to basic authentication with username and password, administrators can use authentication with an API token. This is useful for automation of Awingu through scripts using the REST API. As this token never expires, it is recommended to limit the usage of the token to the network of the computers/servers where the scripts are running using Whitelisted Subnets.

Note: if Whitelisted Subnets is disabled for API Token Based Authentication, the API token can be used from anywhere.

Administrators can generate an API token from their **Account settings** page under **Manage API token**:



When automating the configuration by means of a REST API, it is possible to use a token to bypass logging in and the multi-factor authentication: you will not be prompted to fill in a username and password.

Only administrators can generate a token for their username. When generating a new token, the previous token is disabled.

Please refer to the Administration Manual for more information about REST API-based configuration.

Warning: A token is equivalent to a password and should therefore be kept secret. Anyone with a token has the same access rights and configuration permissions as the user who generated it.

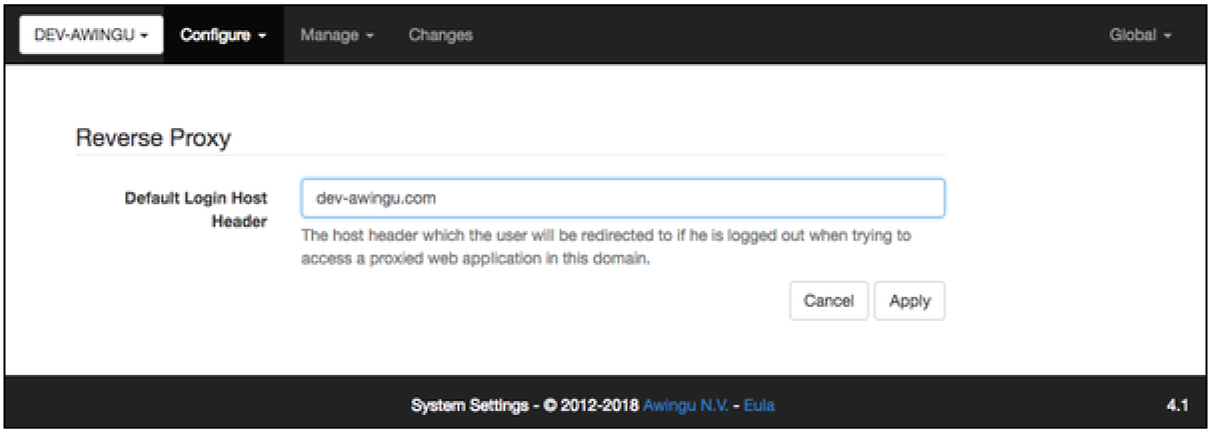
Please enter your password to generate or disable a token:

Password

Generated token for dev-awingu\kerwyny:

See Automate Awingu via the REST API for a PowerShell example.

Reverse Proxy



Default Login Host Header: dev-awingu.com

The host header which the user will be redirected to if he is logged out when trying to access a proxied web application in this domain.

System Settings - © 2012-2018 Awingu N.V. - Eula 4.1

Here you set the default host header for this domain that will be used when accessing a reverse-proxied web application.

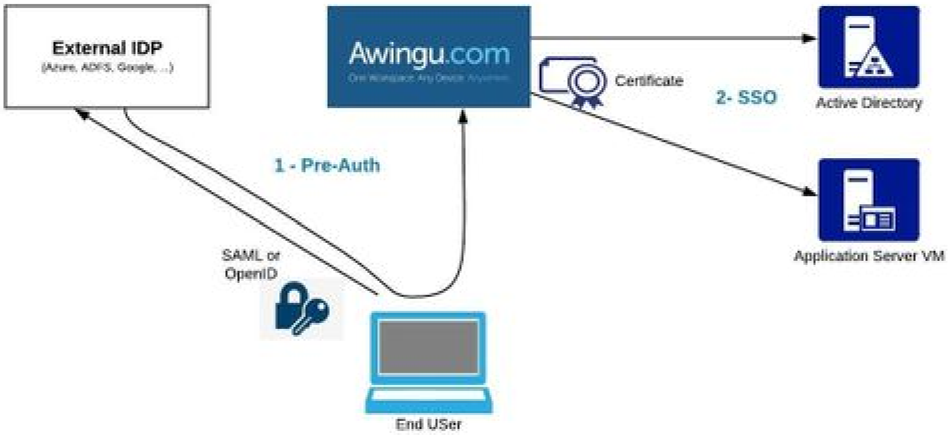
Federated Authentication

ℹ See Awingu Single Sign On (SSO) for detailed instructions on how to setup Single Sign-On and SAML/OpenID connect Authentication.

Next to the standard username/password login, Awingu is also able to do a full Single Sign-on (SSO) via an external Identity Provider.

When switching to *SSO* the login becomes a 2 step process.

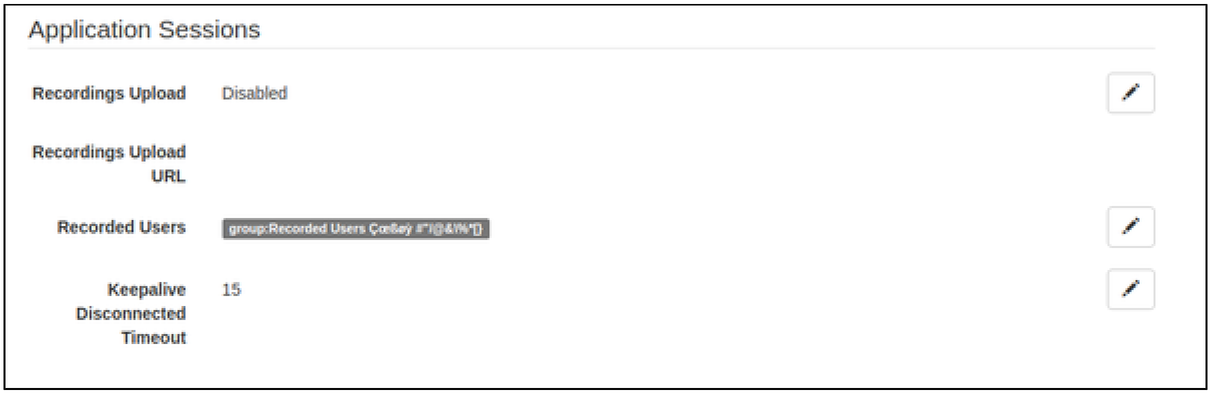
Firstly Awingu no longer does the authentication of the user itself, but this is handled by an external Identity Provider (IDP). As the external IDP doesn't expose the passwords and the Microsoft Remote Desktop Protocol (RDP) doesn't support ticket/token based logins, in a second step, the credential based logins towards back-end systems (remote app, VDI, storage, ...) is replaced by a certificate based login mechanism.



Enabling the Federated Authentication can be done in 2 steps/levels:

1. When enabling Pre-Authentication, the user will need to authenticate with the configured identity provider before authenticating in Awingu. This adds an additional validation steps but will still require that the user provides his Windows password to the Awingu Appliance. See Enabling Pre-Authentication (PreAuth) for integration instructions.
2. Once Pre-Authentication is working, the password step can be replaced by a full Single Sign-On process based on certificate/kerberos login mechanism. See Enable Single Sign-On (SSO) for integration instructions.

Application Sessions



Application Sessions

Recordings Upload	Disabled
Recordings Upload URL	
Recorded Users	group:Recorded Users Çœßøÿ #"!@&%*{}
Keepalive Disconnected Timeout	15

This section applies to streamed applications (RDP apps and RemoteApps).

Application Recording

Awingu allows to save recordings of streamed application sessions. When a session recording ends, the resulting recording file is automatically transferred from the Awingu appliance local disk to a back-end server you can define. Those recording files can be played with the **Recorded Session Player**, which is accessible for all users in a group with the *admin* label.

When this feature is enabled, following streamed app sessions will be recorded:

- All Applications with the *record* label (cf. Application Management)
- All users defined by the labels in the **Recorded Users** setting.

Settings:

- **Recordings Upload**: Enable or disable the feature to record sessions for streamed applications
- **Recordings Upload URL**: Specifies destination for recorded sessions in following specific structure:
  - For HTTP: http://username:password@server:port/path/to/save
  - For SMB/CIFS: smb://DOMAIN\username:password@server:port/path/to/save
    Note that DOMAIN should match an Awingu domain name, which might be different from the NetBIOS name, and must be upper case.

- For privacy reasons, please make sure that only authorized personnel can access the server defined in Recordings Upload URL.
- Known issue: certain special characters in the password are not allowed.

Session keep-alive

A streamed application sessions can be kept alive when the end user accidentally close their browser or browser tab, when they loose network connectivity or when they logout without closing their applications.

Keepalive Disconnected Timeout: Number of minutes the session will be kept alive. After the time-out, the application will be terminated (unsaved changes will be lost). The maximum value is 1440 minutes (1 day).

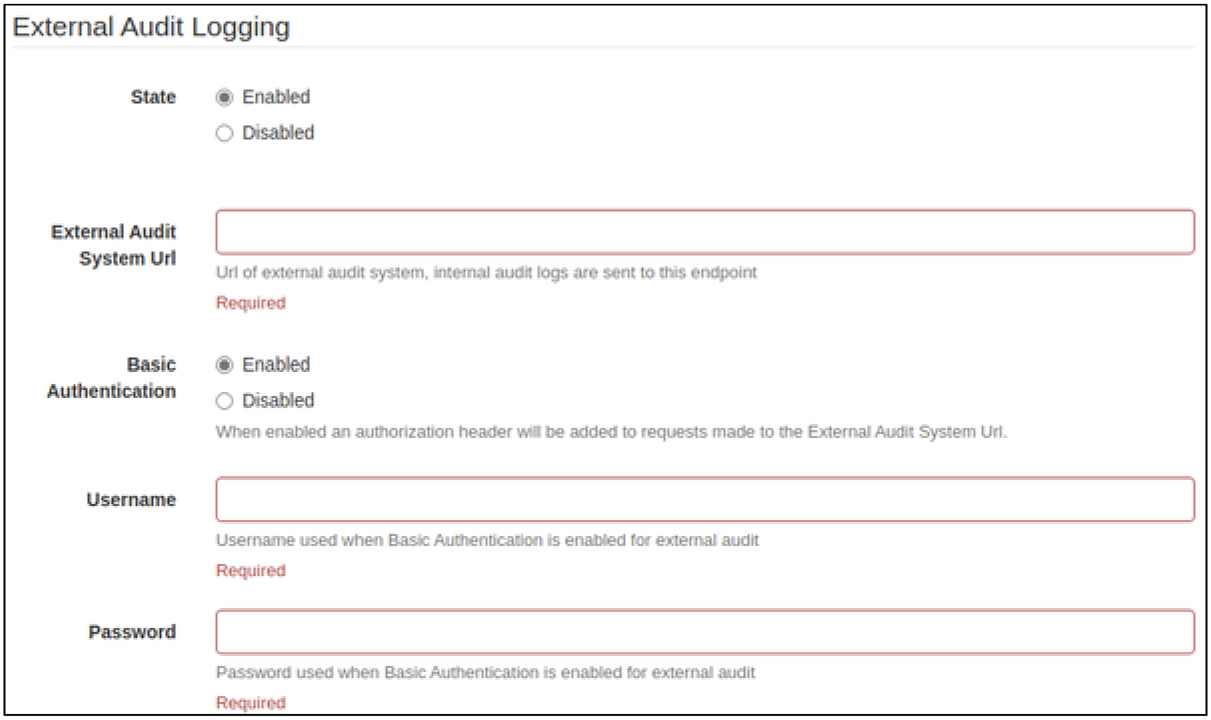
External Audit Logging

Awingu allows you to forward all audit logs to an external system using the HTTP protocol.

This can be used to integrate Awingu with external systems such as security tools (e.g. SIEM tools), reporting tools or automation systems.

This functionality can only be used when the audit logs are migrated to the DB on Awingu 5.0

To enable audit log forwarding, only a URL is required, optionally you can provide credentials for Basic Authentication.



External Audit Logging

State ● Enabled ○ Disabled

External Audit System Url

Url of external audit system, internal audit logs are sent to this endpoint

Required

Basic Authentication ● Enabled ○ Disabled

When enabled an authorization header will be added to requests made to the External Audit System Url.

Username

Username used when Basic Authentication is enabled for external audit

Required

Password

Password used when Basic Authentication is enabled for external audit

Required

- **State:** Enable or disable the forwarding of audit logs for this domain
- **External Audit System URL:** The URL whereto all audit logs will be forwarded.
- **Basic Authentication:** Enable to add an authorization header to all requests with the specified credentials
- **Username:** (Optional) Username to use for Basic Authentication
- **Password:** (Optional) Password to use for Basic Authentication

More information on how you can integrate *External Audit Logging* can be found on External Audit Logging

System Settings - Manage

Domain specific objects can be managed here:

- Application Management
- Application Server Management
- Category Management
- Drive Management
- File Type Management
- Label Management
- User Management

Application Management

Introduction

This page allows to manage applications for each domain. Awingu supports following types of applications:

- Streamed Applications, using the Remote Desktop Protocol. Awingu supports 3 flavors:
  - **RDP Application**: will make use of the regular Remote Desktop Protocol.
  - **Desktop Application**: similar to the RDP Application type except that the Command, Working Folder and File Types properties do not have to be provided.
  - **Remote Application**: an extension to the Remote Desktop Protocol. RemoteApp needs to be supported by your application server, and your applications need be exposed over RemoteApp. It have has several advantages over the regular RDP applications:
    - The window selector (Windows button in the top of the app) is available.
    - The experience on tablets is smoother (especially when rotating the tablet and zooming in/out).
    - The app sharing experience is better.
    - It uses less resources on the application server.

  > When both RemoteApp as RDP Applications are supported on your application server, we strongly recommend to use RemoteApp.

- Web Applications. Web applications are not served through the RDP gateway. Instead when launching a web application, a separate browser tab will be opened. You can specify whether to use the **built-in reverse proxy** for HTTP(S).
  - **Web Application**: The browser will be redirected directly to the URL of the web application, which needs to reachable from the end-user's device.
  - **Reverse Proxied Web Application**:
    - The browser will be redirected to a configured source hostname (e.g. intranet.mycompany.com), which resolves (through DNS) to the same IP as the Awingu environment.
    - Awingu will check if the user is authenticated and has right to access the application. If so, the content of the web application is reverse proxied through Awingu.
    - Awingu can be configured to rewrite HTTP headers (including cookies) and the body to replace all occurrences of the destination URL with the source hostname.
    - If Awingu is configured to do SSL offloading, it also behaves as an SSL offloader for an HTTP web application.
    - If the web application supports Basic Authentication, the username and password given to Awingu can be provided to the web application (= Single Sign-On, SSO).

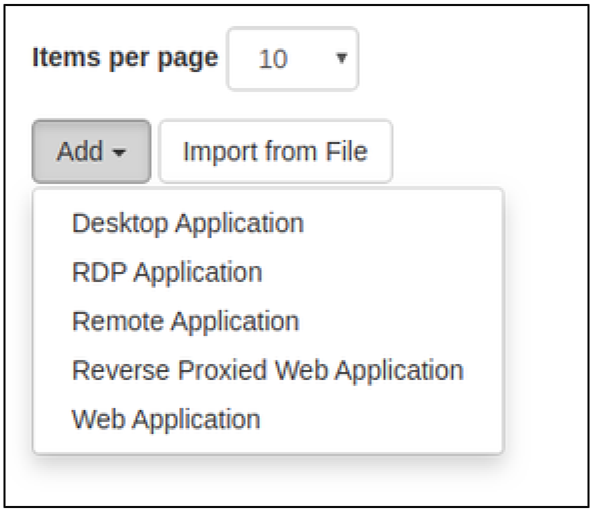
    The technical flow of opening a reverse proxied web application is documented here. There are however some limitations:
    - When the rewrite option is enabled, the web application might still have links to the original destination URL instead of the configured source hostname. This might be because it uses content that is not text/html or because the URL is obfuscated or encoded. Therefore, if the web application has support to run behind a reverse proxy, we recommend to not use the rewrite option in that case.
    - The reverse proxy uses a connection pool towards the web application. This means NTLM authentication cannot work because it needs a persistent connection to the browser.
    - Uploading a file to a reverse proxied web application is limited to 100mb.

Other references:

- To define the application servers, please refer to Application Server Management.
- To prepare the application servers, please refer to Integrating with existing Windows environment.
- Awingu does NOT manage the actual applications on the application server(s). There are commercial products are available to do so.

Adding applications manually

Click on **Add** and choose the type of application you would like to add.

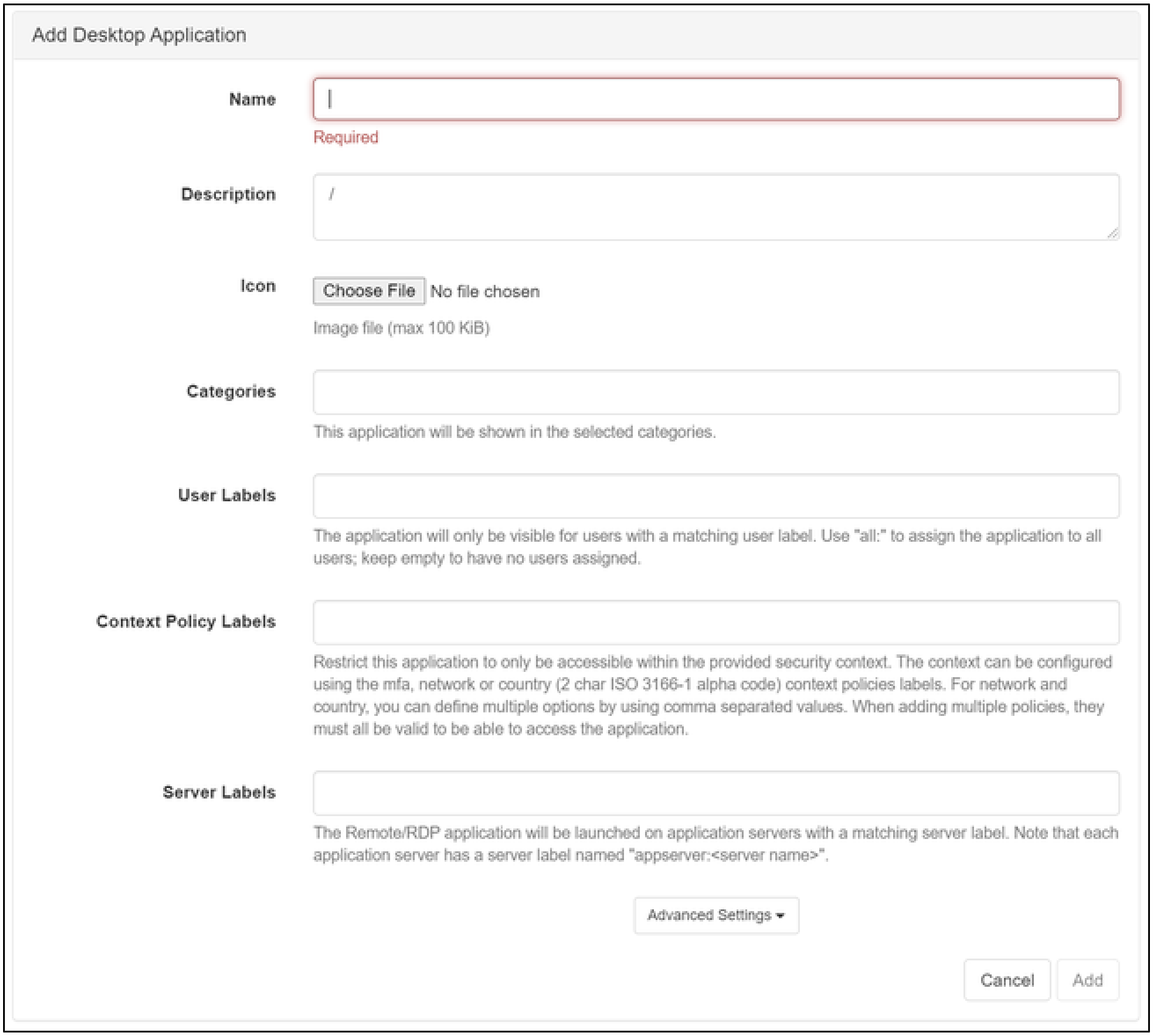


General Settings

The following general settings apply to all types of applications:

- **Name**: The application name as it will appear in the Awingu user interface.
- **Description**: description of the application, not visible to end-users.
- **Icon**: The application icon that will be visible to the end-user in the Awingu user interface. When you upload an icon, it is saved to the database and automatically propagated to all Awingu front-end instances in your Awingu deployment. Only ICO, JPG and PNG are allowed.
- **Categories**: Associate zero, one or more application categories to this application.
- **User Labels**: User labels are used in the process of authorizing users to applications. Only users with labels assigned in this field will see the application in the Applications tab (use *all*: to be visible for all users). See chapter on Label Management for more information.
- **Shown in Applications:** When disabled, the application will not be shown on the Applications page in Awingu. Note: This only hides the application. If the user has the appropriate permissions for the application, he will still be able to access the application via the Direct link.
- **Labels**: Add labels to applications to group them. These groups can be used to filter application servers in lists and reports. This is also used to enable specific features:
  - The *smartcard:* label is used to enable smart card access for this application (see Smart Card Redirection for more information).
  - The *record:* label is used to to activate session recording for this application for all users (needs to be enabled).
  - The *rewritegroup:xxxxx* label is useful when multiple web applications are reverse proxied by Awingu and are linking to each other. By default Awingu will only rewrite URLs per reverse proxy web application. Note: make sure to first create this label in Manage > Labels.
- **Auto Start Labels:** Start the application automatically at login for users with defined matching labels. The set of labels you can define, are the same as *User Labels*. Use "all:" to enable auto start of the application for all users. The application will be started in the background and will be available to the user via the sidebar. Note: recorded applications will not be started automatically and this feature is not compatible with the option Ask for Credentials.

Desktop Application


Add Desktop Application

Name | Required

Description

Icon — Choose File No file chosen

Image file (max 100 KiB)

Categories

This application will be shown in the selected categories.

User Labels

The application will only be visible for users with a matching user label. Use "all:" to assign the application to all users; keep empty to have no users assigned.

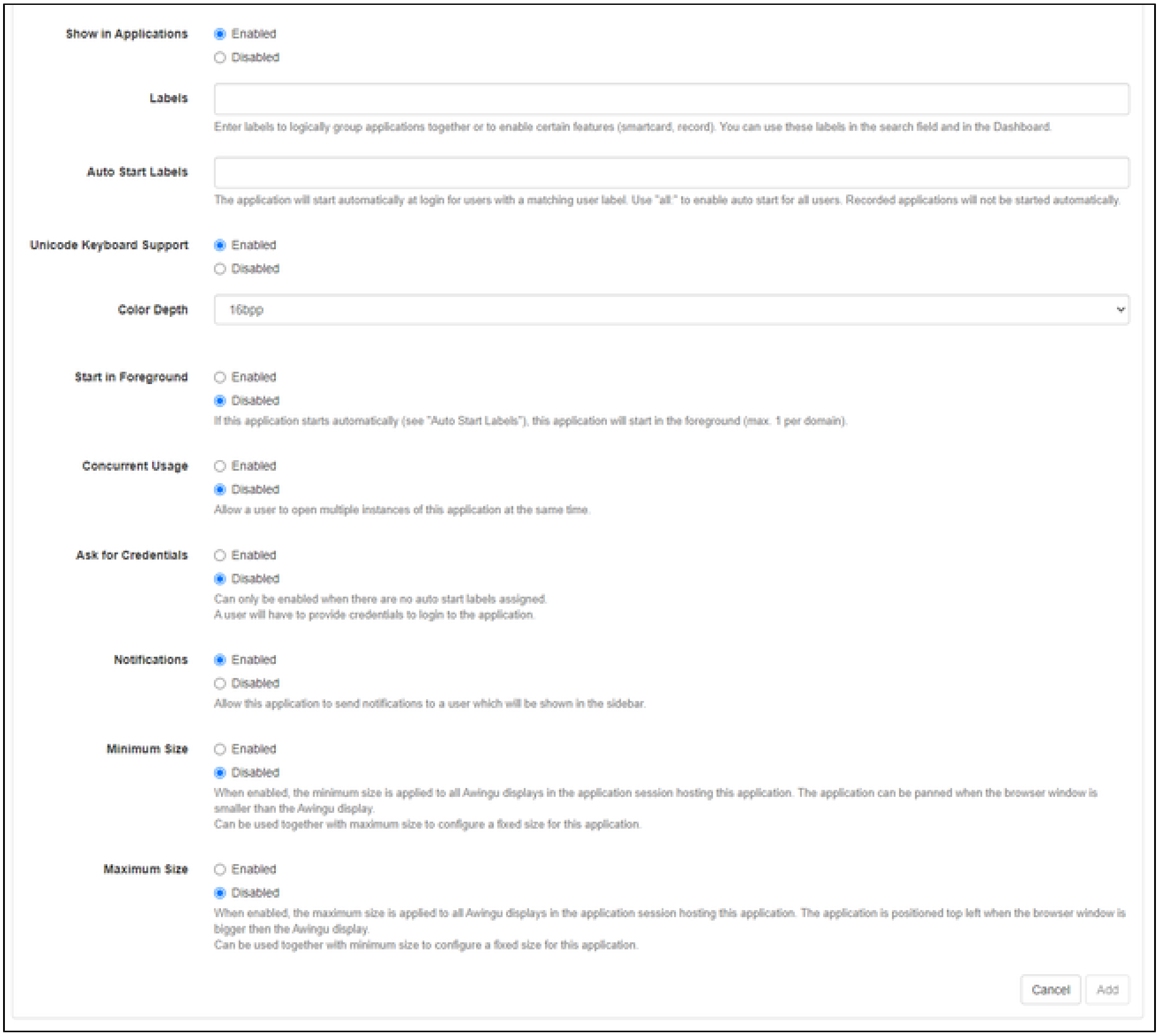
Context Policy Labels

Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application.

Server Labels

The Remote/RDP application will be launched on application servers with a matching server label. Note that each application server has a server label named "appserver:<server name>".

- **Server Labels:** Server labels identify on which application servers this application is available. When a users launches this application, these labels will be used to define a list of applicable servers to connect to.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.



Show in Applications
● Enabled
○ Disabled

Labels

Enter labels to logically group applications together or to enable certain features (smartcard, record). You can use these labels in the search field and in the Dashboard.

Auto Start Labels

The application will start automatically at login for users with a matching user label. Use "all:" to enable auto start for all users. Recorded applications will not be started automatically.

Unicode Keyboard Support
● Enabled
○ Disabled

Color Depth: 16bpp

Start in Foreground
○ Enabled
● Disabled

If this application starts automatically (see "Auto Start Labels"), this application will start in the foreground (max. 1 per domain).

Concurrent Usage
○ Enabled
● Disabled

Allow a user to open multiple instances of this application at the same time.

Ask for Credentials
○ Enabled
● Disabled

Can only be enabled when there are no auto start labels assigned.
A user will have to provide credentials to login to the application.

Notifications
● Enabled
○ Disabled

Allow this application to send notifications to a user which will be shown in the sidebar.

Minimum Size
○ Enabled
● Disabled

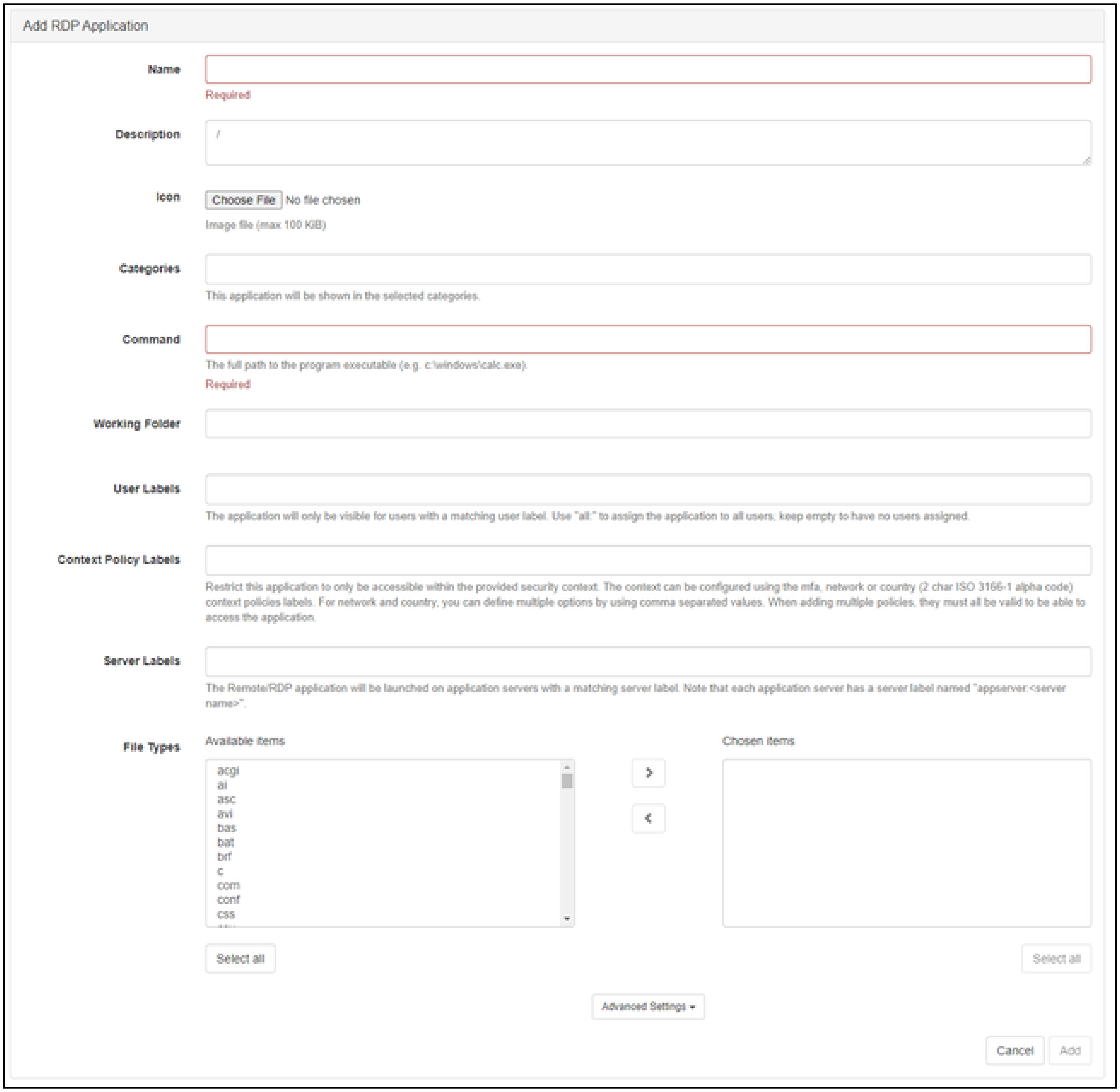
When enabled, the minimum size is applied to all Awingu displays in the application session hosting this application. The application can be panned when the browser window is smaller than the Awingu display.
Can be used together with maximum size to configure a fixed size for this application.

Maximum Size
○ Enabled
● Disabled

When enabled, the maximum size is applied to all Awingu displays in the application session hosting this application. The application is positioned top left when the browser window is bigger then the Awingu display.
Can be used together with minimum size to configure a fixed size for this application.

- **Unicode Keyboard Support**: Disable when the application (e.g. software made with Qt) does not support the Unicode Keyboard that Awingu uses in the RDP Gateway. We suggest first to try with Unicode Keyboard Support enabled: when typing in the application results in a repetition of the first typed character (or other odd behavior), then you should disable the Unicode support. The advantage of Unicode Keyboard is better recognition of special characters on keyboards and the use of on-screen keyboards on tablets.
- **Color Depth:** Defines how many bits per pixels should be used. The higher the color depth, the higher the detail of the application but it will also take more processing and bandwidth. Default set at 16bpp and can be increased to 24bpp or 32bpp.
- **Start in Foreground***:* If enabled and the application auto starts at login, it will immediately be presented to the user and the workspace will be skipped.
- **Concurrent Usage**: Allow a user to open multiple instances of this application at the same time. This is enabled by default. A common use case to disable this option is for an application that accesses a predefined user-owned file, like Microsoft Outlook (only one process can access the user's mailbox).
- **Ask for Credentials***:* A user will have to provide credentials to login to the application (otherwise Awingu provides the login credentials to the application server). This is useful when the Server Labels are linked to application servers that are not joined to the Windows domain. Can only be enabled when there are no Auto Start Labels assigned.
- **Notifications:** Allow this application to send notifications to a user (default enabled). Those notifications will be shown in the sidebar as a red dot. If the application provides a relevant hover text for the systray icon, this will also be shown to the user.
- **Minimum Size**: When enabled, you can set a minimum size to be able to use this application on devices with small screens. If the visible part of the application session is smaller than this minimum size, you will be able to pan inside the session.
- **Maxium Size:** When enabled, you can set a maximum size of the application. When the browser window is bigger than the application, the application will be positioned in the top left. Can be used together with the minimum size feature to configure a fixed size for this application.

RDP Application



Add RDP Application

Name

Required

Description

Icon

Image file (max 100 KiB)

Categories

This application will be shown in the selected categories.

Command

The full path to the program executable (e.g. c:\windows\calc.exe).

Required

Working Folder

User Labels

The application will only be visible for users with a matching user label. Use "all:" to assign the application to all users; keep empty to have no users assigned.

Context Policy Labels

Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application.

Server Labels

The Remote/RDP application will be launched on application servers with a matching server label. Note that each application server has a server label named "appserver:<server name>".

File Types

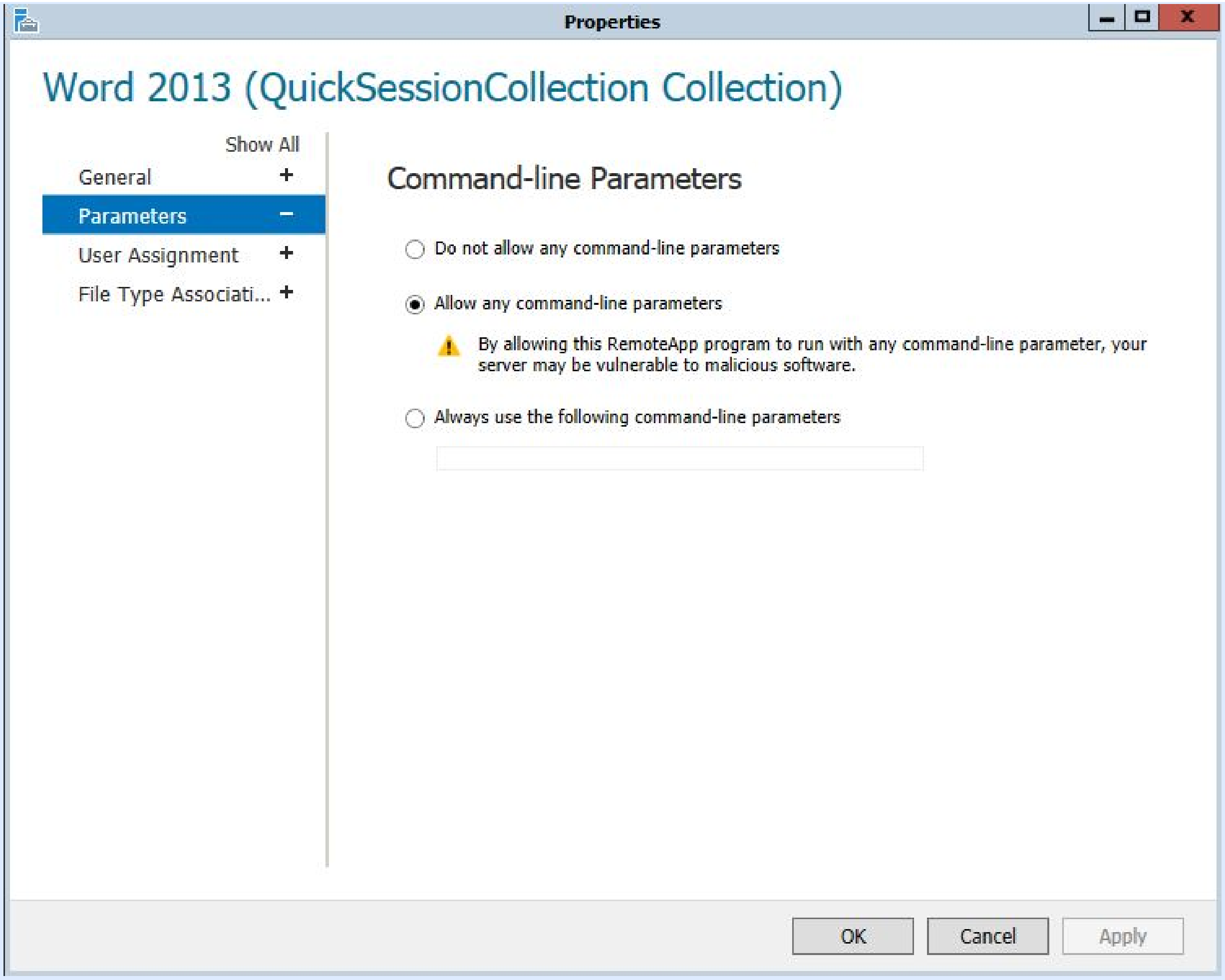
Available items

acgi
ai
asc
avi
bas
bat
brf
c
com
conf
css

Chosen items

- **Command**: The full path to the program executable.
- **Working Folder**: Folder into which an application needs to be launched, i.e. the current working directory. This can remain empty.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.
- **Server Labels:** Server labels identify on which application servers this application is available. When a users launches this application, these labels will be used to define a list of applicable servers to connect to.
- **File Types:** Associate zero, one or multiple file types with this application for viewing or editing.

> If you want to associate file types with applications, such that you can open files with a linked application when clicking on the file, you need to make a few additional configuration steps:
>
> 1. On your application server, make sure you have enabled the option **"Allow any command-line arguments"** for your remoteapp.



Command-line Parameters

○ Do not allow any command-line parameters

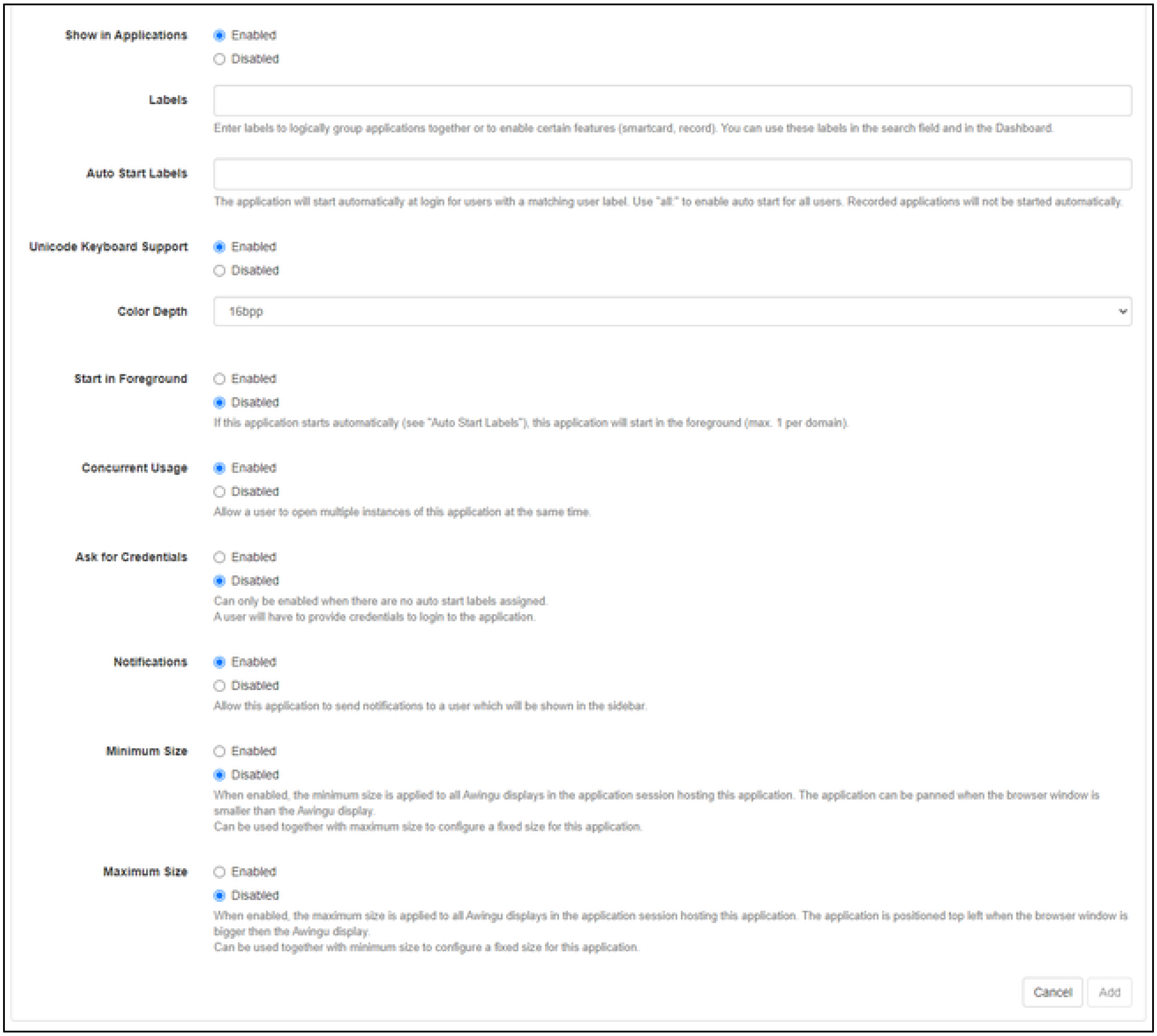
● Allow any command-line parameters

⚠ By allowing this RemoteApp program to run with any command-line parameter, your server may be vulnerable to malicious software.

○ Always use the following command-line parameters

2. Make sure you have included the **'document' placeholder** into the UNC path of your drives Drive Management

When you configure file types for MS Excel, make sure you also add the two "openxmlformat-officedocument.spreadsheet" media types. This is required for opening ".xlsx" files.



Show in Applications
● Enabled
○ Disabled

Labels
Enter labels to logically group applications together or to enable certain features (smartcard, record). You can use these labels in the search field and in the Dashboard.

Auto Start Labels
The application will start automatically at login for users with a matching user label. Use "all:" to enable auto start for all users. Recorded applications will not be started automatically.

Unicode Keyboard Support
● Enabled
○ Disabled

Color Depth
16bpp

Start in Foreground
○ Enabled
● Disabled
If this application starts automatically (see "Auto Start Labels"), this application will start in the foreground (max. 1 per domain).

Concurrent Usage
● Enabled
○ Disabled
Allow a user to open multiple instances of this application at the same time.

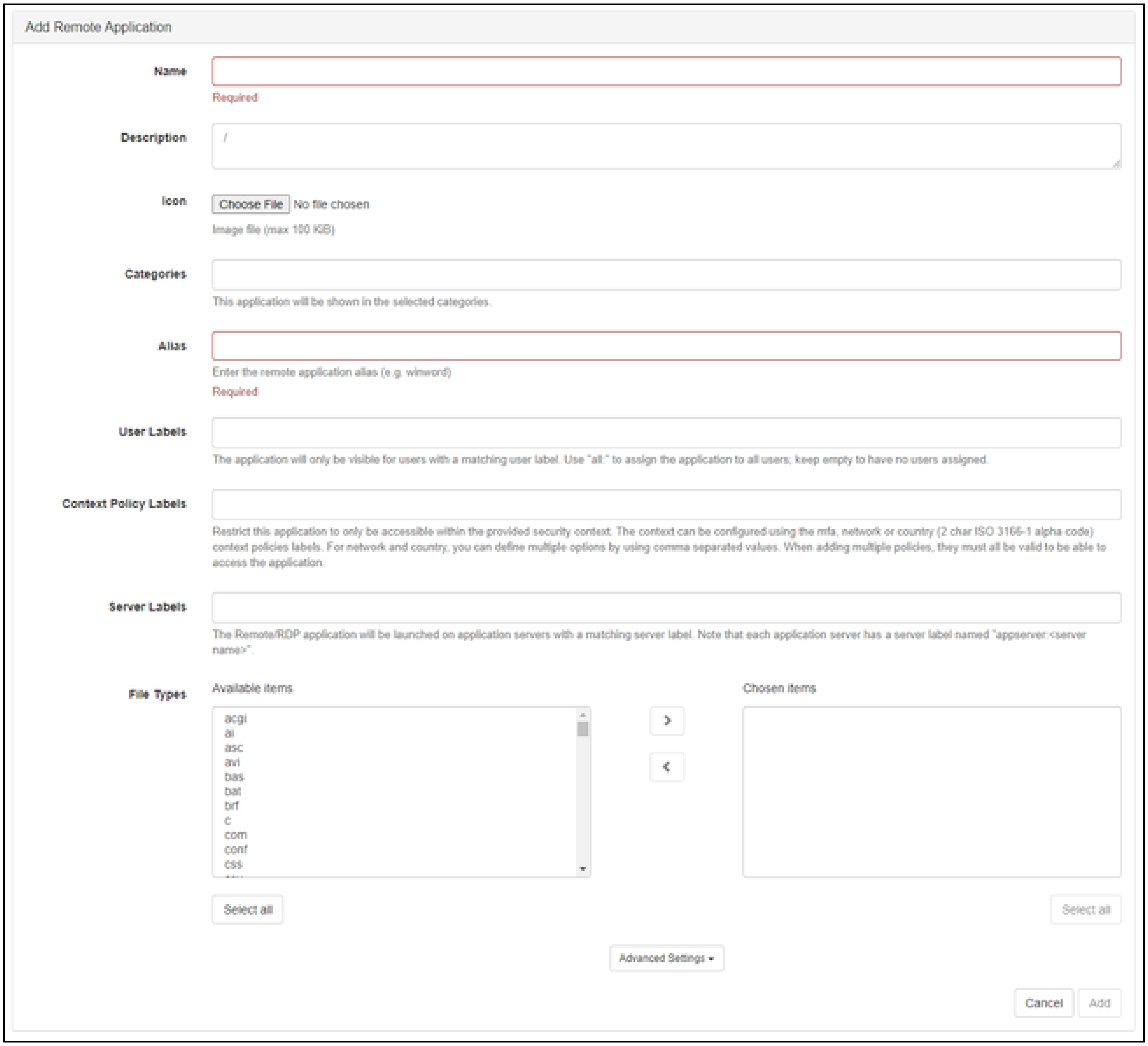
Ask for Credentials
○ Enabled
● Disabled
Can only be enabled when there are no auto start labels assigned.
A user will have to provide credentials to login to the application.

Notifications
● Enabled
○ Disabled
Allow this application to send notifications to a user which will be shown in the sidebar.

Minimum Size
○ Enabled
● Disabled
When enabled, the minimum size is applied to all Awingu displays in the application session hosting this application. The application can be panned when the browser window is smaller than the Awingu display.
Can be used together with maximum size to configure a fixed size for this application.

Maximum Size
○ Enabled
● Disabled
When enabled, the maximum size is applied to all Awingu displays in the application session hosting this application. The application is positioned top left when the browser window is bigger then the Awingu display.
Can be used together with minimum size to configure a fixed size for this application.

- **Unicode Keyboard Support**: Disable when the application (e.g. software made with Qt) does not support the Unicode Keyboard Awingu uses in the RDP Gateway. We suggest first to try with Unicode Keyboard Support enabled: when typing in the application results in a repetition of the first typed character (or other odd behavior), then you should disable the Unicode support. The advantage of Unicode Keyboard is better recognition of special characters on keyboards and the use of on-screen keyboards on tablets.
- **Color Depth:** Defines how many bits per pixels should be used. The higher the color depth, the higher the detail of the application but it will also take more processing and bandwidth. Default set at 16bpp and can be increased to 24bpp or 32bpp.
- **Start in Foreground***:* If enabled and the application auto starts at login, it will immediately be presented to the user and the workspace will be skipped.
- **Concurrent Usage**: Allow a user to open multiple instances of this application at the same time. This is enabled by default. A common use case to disable this option is for an application that accesses a predefined user-owned file, like Microsoft Outlook (only one process can access the user's mailbox).
- **Ask for Credentials***:* A user will have to provide credentials to login to the application (otherwise Awingu provides the login credentials to the application server). This is useful when the Server Labels are linked to application servers that are not joined to the Windows domain. Can only be enabled when there are no Auto Start Labels assigned.
- **Notifications:** Allow this application to send notifications to a user (default enabled). Those notifications will be shown in the sidebar as a red dot. If the application provides a relevant hover text for the systray icon, this will also be shown to the user.
- **Minimum Size**: When enabled, you can set a minimum size to be able to use this application on devices with small screens. If the visible part of the application session is smaller than this minimum size, you will be able to pan inside the session.
- **Maxium Size:** When enabled, you can set a maximum size of the application. When the browser window is bigger than the application, the application will be positioned in the top left. Can be used together with the minimum size feature to configure a fixed size for this application.



Add Remote Application

Name

Required

Description

Icon

No file chosen

Image file (max 100 KiB)

Categories

This application will be shown in the selected categories.

Alias

Enter the remote application alias (e.g. winword)

Required

User Labels

The application will only be visible for users with a matching user label. Use "all:" to assign the application to all users; keep empty to have no users assigned.

Context Policy Labels

Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application.

Server Labels

The Remote/RDP application will be launched on application servers with a matching server label. Note that each application server has a server label named "appserver:<server name>".

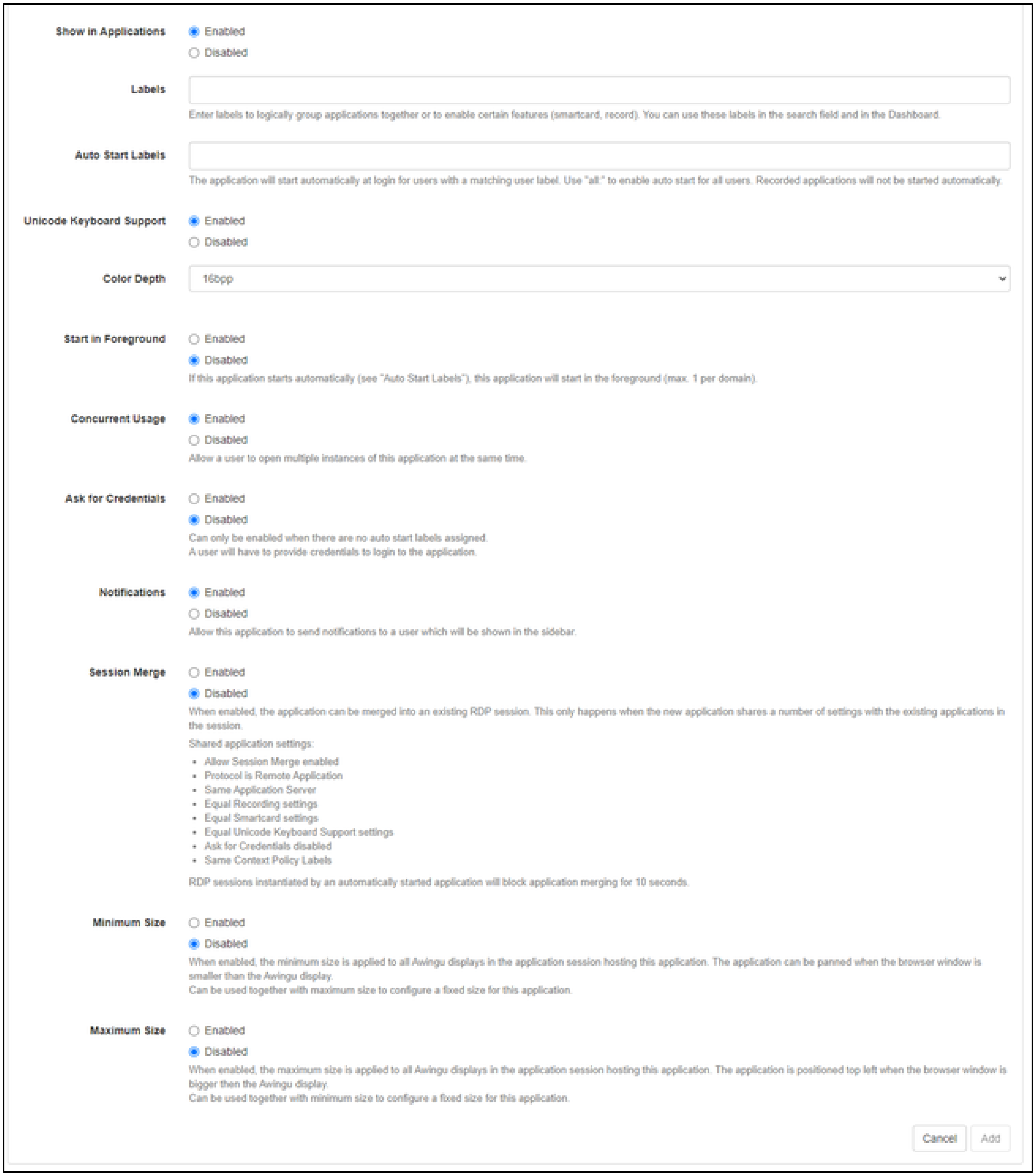
File Types

Available items

acgi
ai
asc
avi
bas
bat
brf
c
com
conf
css

Chosen items

- **Alias**: Provide the Remote Application alias.
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.
- **Server Labels:** Server labels identify on which application servers this application is available. When a users launches this application, these labels will be used to define a list of applicable servers to connect to.
- **File Types**: Associate zero, one or multiple file types with this application for viewing or editing. See the RDP File Types property above for additional information.



Show in Applications
● Enabled
○ Disabled

Labels

Enter labels to logically group applications together or to enable certain features (smartcard, record). You can use these labels in the search field and in the Dashboard.

Auto Start Labels

The application will start automatically at login for users with a matching user label. Use "all:" to enable auto start for all users. Recorded applications will not be started automatically.

Unicode Keyboard Support
● Enabled
○ Disabled

Color Depth 16bpp

Start in Foreground
○ Enabled
● Disabled
If this application starts automatically (see "Auto Start Labels"), this application will start in the foreground (max. 1 per domain).

Concurrent Usage
● Enabled
○ Disabled
Allow a user to open multiple instances of this application at the same time.

Ask for Credentials
○ Enabled
● Disabled
Can only be enabled when there are no auto start labels assigned.
A user will have to provide credentials to login to the application.

Notifications
● Enabled
○ Disabled
Allow this application to send notifications to a user which will be shown in the sidebar.

Session Merge
○ Enabled
● Disabled
When enabled, the application can be merged into an existing RDP session. This only happens when the new application shares a number of settings with the existing applications in the session.

Shared application settings:

- Allow Session Merge enabled
- Protocol is Remote Application
- Same Application Server
- Equal Recording settings
- Equal Smartcard settings
- Equal Unicode Keyboard Support settings
- Ask for Credentials disabled
- Same Context Policy Labels

RDP sessions instantiated by an automatically started application will block application merging for 10 seconds.

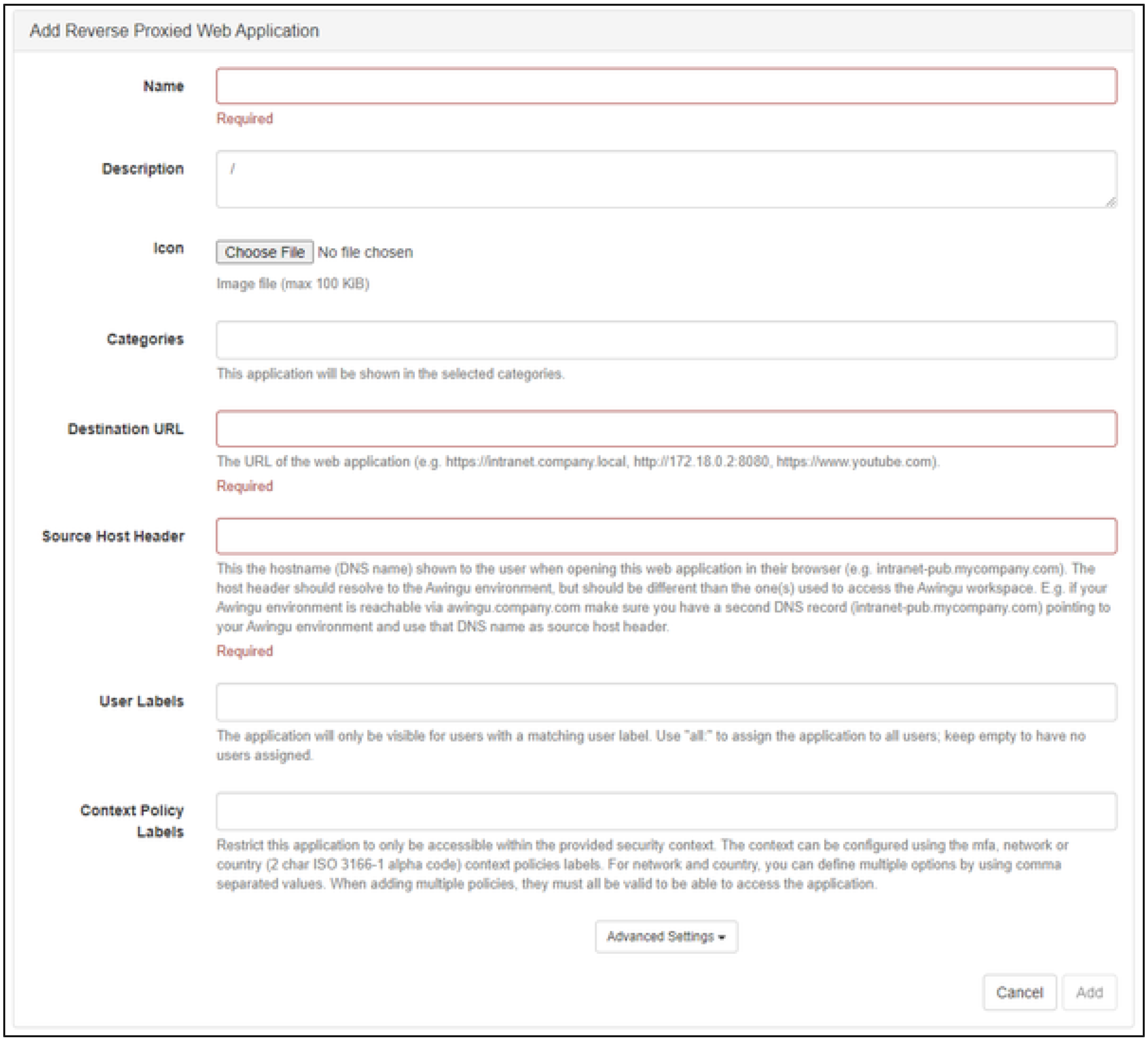
Minimum Size
○ Enabled
● Disabled
When enabled, the minimum size is applied to all Awingu displays in the application session hosting this application. The application can be panned when the browser window is smaller than the Awingu display.
Can be used together with maximum size to configure a fixed size for this application.

Maximum Size
○ Enabled
● Disabled
When enabled, the maximum size is applied to all Awingu displays in the application session hosting this application. The application is positioned top left when the browser window is bigger then the Awingu display.
Can be used together with minimum size to configure a fixed size for this application.

- **Unicode Keyboard Support**: Disable when the application (e.g. software made with Qt) does not support the Unicode Keyboard Awingu uses in the RDP Gateway. We suggest first to try with Unicode Keyboard Support enabled: when typing in the application results in a repetition of the first typed character (or other odd behavior), then you should disable the Unicode support. The advantage of Unicode Keyboard is better recognition of special characters on keyboards and the use of on-screen keyboards on tablets.
- **Color Depth:** Defines how many bits per pixels should be used. The higher the color depth, the higher the detail of the application but it will also take more processing and bandwidth. Default set at 16bpp and can be increased to 24bpp or 32bpp.
- **Start in Foreground***:* If enabled and the application auto starts at login, it will immediately be presented to the user and the workspace will be skipped.
- **Concurrent Usage**: Allow a user to open multiple instances of this application at the same time. This is enabled by default. A common use case to disable this option is for an application that accesses a predefined user-owned file, like Microsoft Outlook (only one process can access the user's mailbox).

- **Ask for Credentials***:* A user will have to provide credentials to login to the application (otherwise Awingu provides the login credentials to the application server). This is useful when the Server Labels are linked to application servers that are not joined to the Windows domain. Can only be enabled when there are no Auto Start Labels assigned.
- **Notifications:** Allow this application to send notifications to a user (default enabled). Those notifications will be shown in the sidebar as a red dot. If the application provides a relevant hover text for the systray icon, this will also be shown to the user.
- **Session Merge**: When enabled, the application can be merged into an existing application session. The merge will only happen when the new application shares a number of settings with the existing applications in the session.
    - Required shared application settings:
        - Allow Session Merge enabled
        - Protocol is Remote Application
        - Same Application Server
        - Equal Recording settings
        - Equal Smartcard settings
        - Equal Unicode Keyboard Support settings
        - Ask for Credentials disabled
        - Same Context Policy labels
        - Same RDS Collection labels
    - Advantages: Applications will start faster and consume less resources on the application server.
    - Side effects:
        - Users will see multiple applications in the same application session when they resize or minimize one of the applications.
        - Applications that are merged will also be shown together in the list of Active Sessions in the sidebar of the user.
        - The color depth setting of the merged application will be ignored.
- **Minimum Size**: When enabled, you can set a minimum size to be able to use this application on devices with small screens. If the visible part of the application session is smaller than this minimum size, you will be able to pan inside the session.
- **Maxium Size:** When enabled, you can set a maximum size of the application. When the browser window is bigger than the application, the application will be positioned in the top left. Can be used together with the minimum size feature to configure a fixed size for this application.

Reverse Proxied Web Application



Add Reverse Proxied Web Application

Name

Required

Description

Icon

No file chosen

Image file (max 100 KiB)

Categories

This application will be shown in the selected categories.

Destination URL

The URL of the web application (e.g. https://intranet.company.local, http://172.18.0.2:8080, https://www.youtube.com).

Required

Source Host Header

This the hostname (DNS name) shown to the user when opening this web application in their browser (e.g. intranet-pub.mycompany.com). The host header should resolve to the Awingu environment, but should be different than the one(s) used to access the Awingu workspace. E.g. if your Awingu environment is reachable via awingu.company.com make sure you have a second DNS record (intranet-pub.mycompany.com) pointing to your Awingu environment and use that DNS name as source host header.

Required

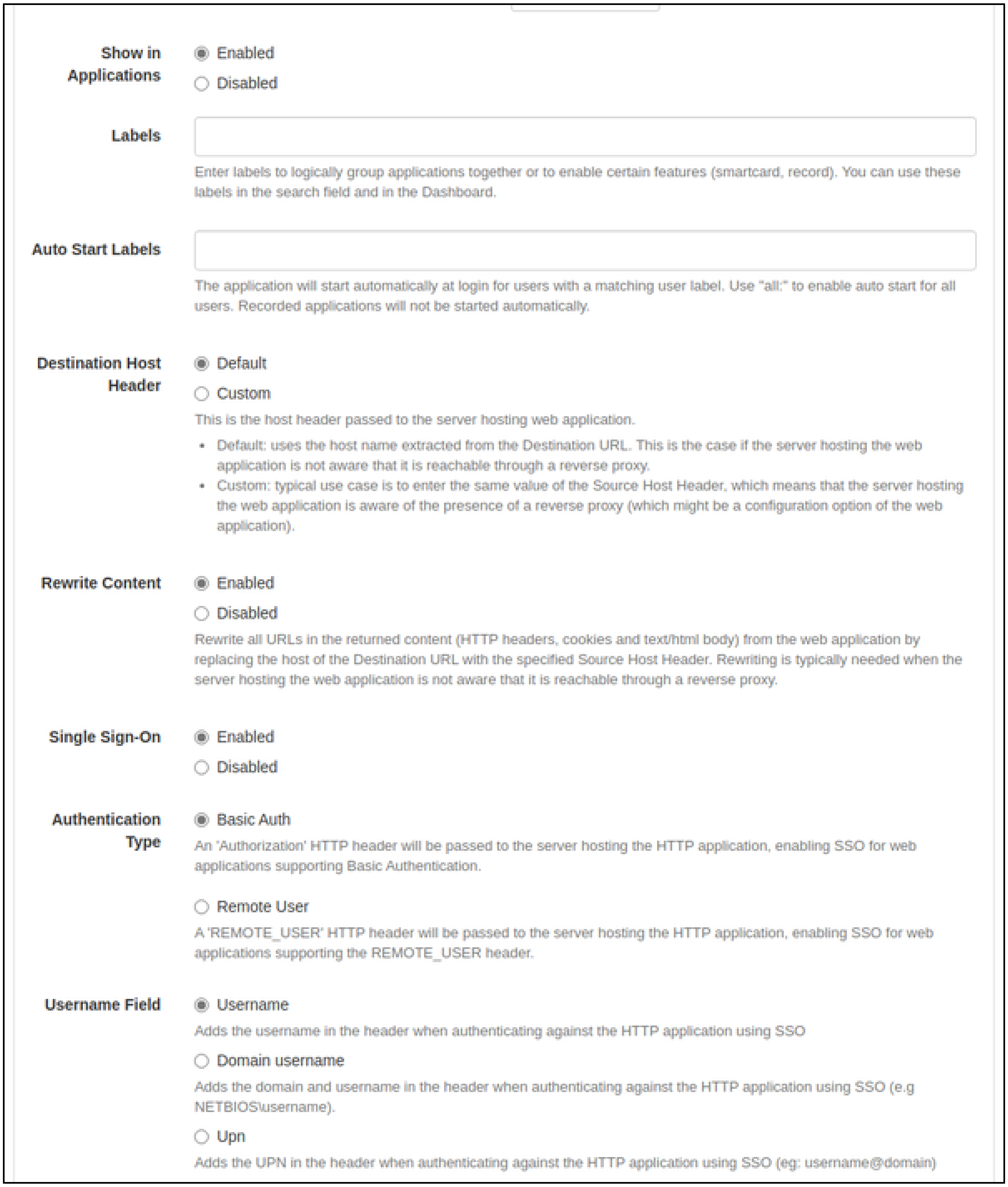
User Labels

The application will only be visible for users with a matching user label. Use "all:" to assign the application to all users; keep empty to have no users assigned.

Context Policy Labels

Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application.

- **Destination URL:** Provide the URL on which the website is reachable for Awingu. Make sure that Awingu is able to access it.
- **Source Host Header:** When a user opens this web application, the Source Host Header will be shown in the URL bar of their browser. This host header should resolve via DNS to the Awingu environment. To increase security, it is recommended not to use a subdomain of the Awingu environment (e.g. don't use intranet.awingu.mycompany.com when awingu.mycompany.com points to your Awingu environment).
- **Context Policy Labels:** Restrict this application to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the application. See the Label Management page for more information and examples.



Show in Applications
● Enabled
○ Disabled

Labels

Enter labels to logically group applications together or to enable certain features (smartcard, record). You can use these labels in the search field and in the Dashboard.

Auto Start Labels

The application will start automatically at login for users with a matching user label. Use "all:" to enable auto start for all users. Recorded applications will not be started automatically.

Destination Host Header
● Default
○ Custom

This is the host header passed to the server hosting web application.

- Default: uses the host name extracted from the Destination URL. This is the case if the server hosting the web application is not aware that it is reachable through a reverse proxy.
- Custom: typical use case is to enter the same value of the Source Host Header, which means that the server hosting the web application is aware of the presence of a reverse proxy (which might be a configuration option of the web application).

Rewrite Content
● Enabled
○ Disabled

Rewrite all URLs in the returned content (HTTP headers, cookies and text/html body) from the web application by replacing the host of the Destination URL with the specified Source Host Header. Rewriting is typically needed when the server hosting the web application is not aware that it is reachable through a reverse proxy.

Single Sign-On
● Enabled
○ Disabled

Authentication Type
● Basic Auth

An 'Authorization' HTTP header will be passed to the server hosting the HTTP application, enabling SSO for web applications supporting Basic Authentication.

○ Remote User

A 'REMOTE_USER' HTTP header will be passed to the server hosting the HTTP application, enabling SSO for web applications supporting the REMOTE_USER header.

Username Field
● Username

Adds the username in the header when authenticating against the HTTP application using SSO

○ Domain username

Adds the domain and username in the header when authenticating against the HTTP application using SSO (e.g NETBIOS\username).

○ Upn

Adds the UPN in the header when authenticating against the HTTP application using SSO (eg: username@domain)

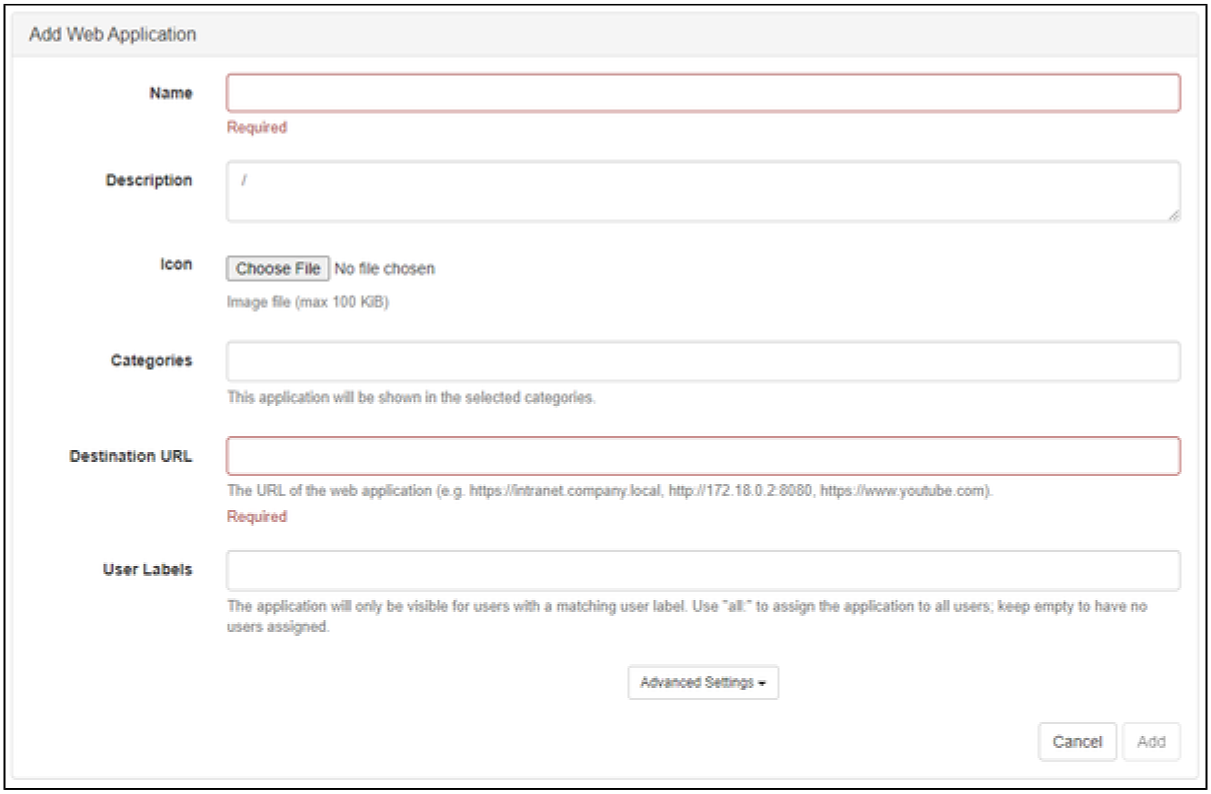
- **Destination Host Header:** This is the host header passed to the web application. By default, the host of the Destination URL is used. If the web application is configured to accept HTTP requests on the Source Host Header, you can use a custom host header (with the same value of the Source Host Header).
- **Rewrite Content:** Rewrite all URLs in the returned content (HTTP headers and cookies and text/html bodies) from the web application by replacing the host of the Destination URL with the specified Source Host Header. If the web application is configured to accept HTTP requests on the Source Host Header, you may need to disable this feature.
- **Single Sign-On**: If enabled the username and password provided when logging in to Awingu will be passed (base64 encoded) to the Web application in a HTTP authorization header. This requires that the Web application supports basic authentication and is hosted on a Web server with basic authentication enabled.
- **Authentication Type:** (when Single Sign-on is enabled) defines how the user will be authenticated to the reverse proxied web application
  - Basic Auth: provide the user's credentials to the reverse proxied application using *Basic Authentication.*
  - Remote User: provide the user's username to the reverse proxied web application using the REMOTE_USER header.
- **Username field:** (when Single Sign-on is enabled) defines the format of the username used to authenticate the user to the reverse proxied web application using the selected *Authentication Type*
  - Username: use the username without domain

- Domain username: use the username prefixed with the domain (e.g. NETBIOS\username)
- Upn: use the UPN of the user as username

Support

- Built-in Reverse Proxy: Rewrite of host headers only works if the URL is clearly present in the body or the headers.
- Unable to make Cross Origin Requests to grouped reverse proxied web applications
- Support for websockets for reverse proxied web applications has been added since the 5.0.0 release.

Web Application



Add Web Application

Name

Required

Description

Icon

No file chosen

Image file (max 100 KiB)

Categories

This application will be shown in the selected categories.

Destination URL

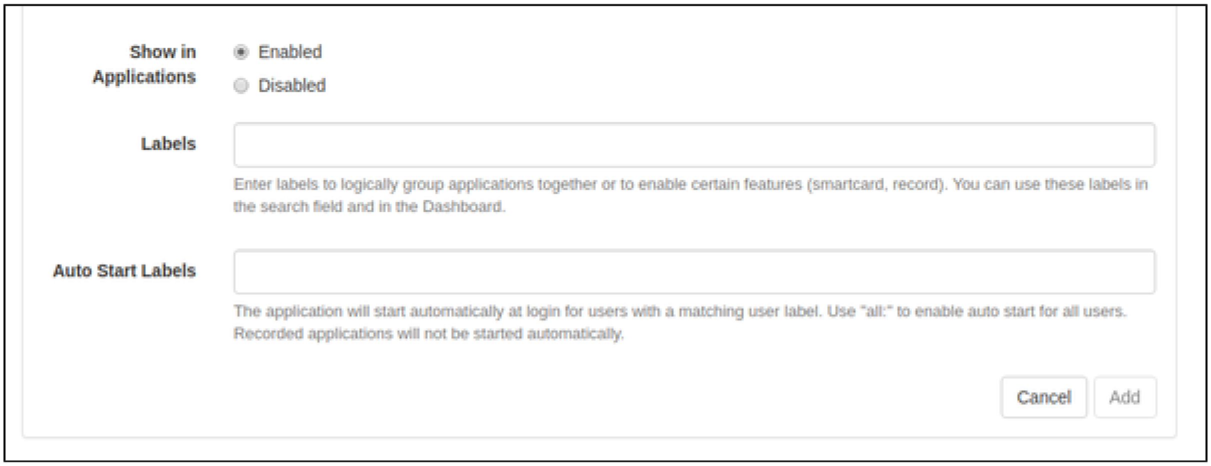
The URL of the web application (e.g. https://intranet.company.local, http://172.18.0.2:8080, https://www.youtube.com).

Required

User Labels

The application will only be visible for users with a matching user label. Use "all:" to assign the application to all users; keep empty to have no users assigned.

- **Destination URL:** Provide the URL on which the website is reachable for the end-user. Make sure the end-user is able to access it.



Show in Applications
● Enabled
○ Disabled

Labels

Enter labels to logically group applications together or to enable certain features (smartcard, record). You can use these labels in the search field and in the Dashboard.

Auto Start Labels

The application will start automatically at login for users with a matching user label. Use "all:" to enable auto start for all users. Recorded applications will not be started automatically.

Importing applications with a CSV file

When importing a CSV (comma separated value) file, you can add multiple applications at once. Only RemoteApp is supported.

The CSV file is formatted as follows:

```
"command","name","icon"
"EXCEL","Microsoft Excel 2010","0,0,1,0,5....."
```

Generating a CSV file

Via a PowerShell script, you can run a script to gather all published RemoteApps on an application server.

1. We provide a sample script on our public GitHub account: https://github.com/Awingu/awingu-utils/blob/master/RemoteApp/PowerShell/get_remoteapps_from_appserver.ps1.
   You can download that script with right-click on the Raw button and save the link content.
2. To run the script, which is not signed, you can open PowerShell and execute:

   ```
   powershell -ExecutionPolicy ByPass -File .
   \get_remoteapps_from_appserver.ps1
   ```

3. The script generates the folder Awingu_Apps in the current working directory containing the CSV file that can be imported in Awingu.

Importing a CSV file

In Awingu, when importing from file, you can configure for all imported applications following fields:

- Categories
- File Types
- Labels
- Server Labels
- User Labels
- Context Policy Labels
- Auto Start Labels
- Unicode Keyboard Support
- Show in Applicatiaons
- Notifications

See Application Management#Adding applications manually for more details about those fields. You can always update the afterwards (via Bulk Action).

Configuring shortcut buttons

For each streamed application, an administrator can configure shortcut buttons that will be provided in a shortcut toolbar to the end user.

Click on the Shortcut Buttons button next to the application name in the list of applications.

Click on Add to create a new key combination:

- **Name**: the text shown on the shortcut button, e.g. Save, Refresh, Next page
- **Key Combination**: text representing the key combination in one of following formats:
  - modifier+key
  - modifier+modifier+key
  - modifier+modifier+modifier+key

Possible modifiers:

- ctrl
- shift
- alt
- altgr
- windows
- context

Possible keys:

- f1 - f12
- a - z
- 0 - 9
- space
- pageup, pagedown
- end, home
- left, up, right, down

- printscreen
- insert
- delete
- esc
- backspace
- tab
- enter

Note: The Remote Desktop Services Shortcut keys are also available in Awingu. See the User Manual for an overview.

Application Server Management

Introduction

When an end-user launches a streamed application, a session is set up dynamically between the Awingu appliance and an application server. A detail of this process, can be found here.

The Application Connector (a component within Awingu) will select the application server (hostname and port) that should be used to set up this connection.

In a typical Awingu environment, there are multiple application servers deployed. An application can be served by one or more application servers. However, it is by no means required that each application is installed on every application server.

It is the role of the application connector to find the most suited application server to launch a particular application at a certain moment in time. The default behavior of the Application Connector is:

1. List all application servers where the application is available (based on server labels).
2. Select the server that has the least open connections (known by the Awingu system).
3. If a server is not reachable, another server from step 1 will be selected.

When using a Application Server Management#Remote Desktop Service Connection Broker (RDS farm), the broker will do the load balancing.

Note: the application servers need to be configured correctly before any streamed application can be opened. Please refer to Integrating with existing Windows environment.

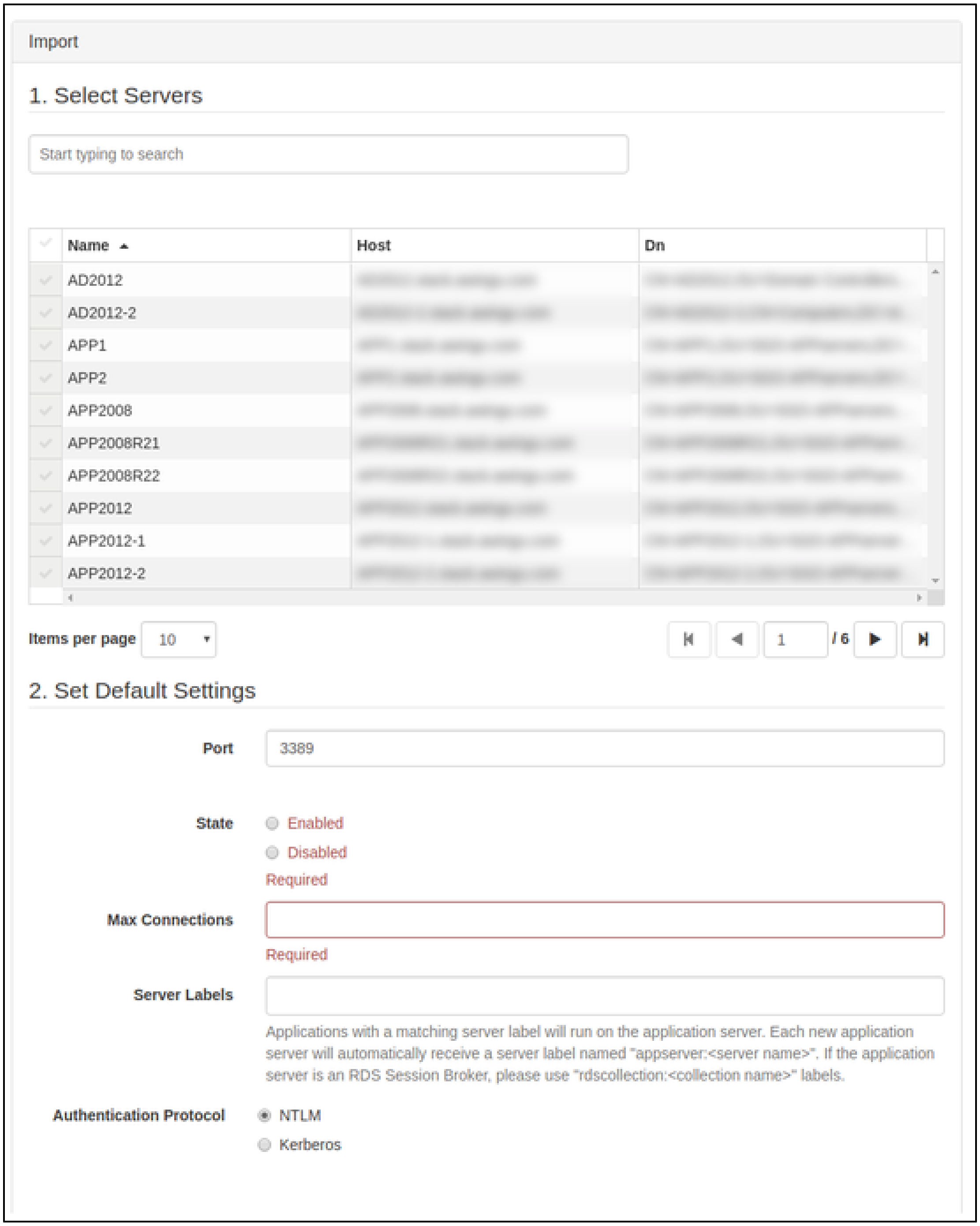
Adding/Configuring Application Servers

Application servers can be added via System Settings > Manage > Application Servers.

Importing application servers

When the bind user has been configured for the domain (see Domain Settings), you can import them by clicking on **Import from AD** and scroll down.

Note: All application servers that are available in the top level domain will be shown. Only domain components (dc=) of the Base DN are used.



Import

1. Select Servers

Start typing to search

Name ▲	Host	Dn
AD2012	[redacted]	[redacted]
AD2012-2	[redacted]	[redacted]
APP1	[redacted]	[redacted]
APP2	[redacted]	[redacted]
APP2008	[redacted]	[redacted]
APP2008R21	[redacted]	[redacted]
APP2008R22	[redacted]	[redacted]
APP2012	[redacted]	[redacted]
APP2012-1	[redacted]	[redacted]
APP2012-2	[redacted]	[redacted]

Items per page: 10 — 1 / 6

2. Set Default Settings

Port: 3389

State: ○ Enabled ○ Disabled
Required

Max Connections:
Required

Server Labels:
Applications with a matching server label will run on the application server. Each new application server will automatically receive a server label named "appserver:<server name>". If the application server is an RDS Session Broker, please use "rdscollection:<collection name>" labels.

Authentication Protocol: ● NTLM ○ Kerberos

1. First select the servers to import. You can use the search box.
2. Configure the servers to import:
    - **Port**: TCP port used to set up the RDP session to the application server (default 3389).
    - **State**: When this attribute is set to 'disabled', no new sessions will be set up to this application server. Toggling from 'enabled' to 'disabled' does not impact active sessions.
    - **Max Connections**: Maximum number of simultaneously active RDP sessions that are allowed to this application server. In case this maximum is reached, no new sessions will be set up to this application server. Note: 0 (zero) results to an unlimited number of connections.
    - **Server Labels**: Add labels to servers to group them. These groups can be used to assign applications (see also Application Management) to servers and to filter application servers in lists and reports.
    - **Authentication Protocol**: Determines which authentication protocol will be used when connecting to the application server (default NTLM). Normally when selecting Kerberos, you need to to provide an authentication host but when your are importing application servers, the authentication host will be set to the host name.

Manually adding/editing application servers

Following attributes can be configured per added application server:

- **Name**: Name of the application server that will be visible in the application connector
- **Host**: Fully qualified domain name or IPv4 of the application server
- **Port**: TCP port used to set up the RDP session to the application server (default 3389).
- **State**: When this attribute is set to 'disabled', no new sessions will be set up to this application server. Toggling from 'enabled' to 'disabled' does not impact active sessions.
- **Max Connections**: Maximum number of simultaneously active RDP sessions that are allowed to this application server. In case this maximum is reached, no new sessions will be set up to this application server. Note: 0 (zero) results to an unlimited number of connections.
- **Description**: Description of the application server (free text format)
- **Server Labels**: Add labels to servers to group them. These groups can be used to assign applications (see also Application Management) to servers and to filter application servers in lists and reports.
- **Authentication Protocol**: Determines which authentication protocol will be used when connecting to the application server (default NTLM). When Kerberos is selected, an **Authentication Host** (FQDN) of the application server is required.

Further Configuration of the Applications

Please refer to Application Management to assign applications to servers and assign applications to users.
This page will also allow you to add applications to categories, define the command that needs to be executed, etc.

Remote Desktop Service Connection Broker

When using the Microsoft Remote Desktop Service Connection Broker (for RDS farm), only the broker needs to be configured in Awingu. The Broker will refer Awingu to the correct application server when opening an application.

1. First create labels in Label Management for each RDS Collection configured on the Broker:
    - Key: *rdscollection*
    - Value: the name of the collection
2. In Application Server Management, add the Broker as an application server. In the *Labels* field, add the labels defined in step 1.
3. In Application Management, when adding an application, use the labels configured in step 1 to assign applications to the collections where they are published.

⚠ When you have changed the name of an RDS collection in the past, you still need to provide the original collection in Awingu. This is because Microsoft Windows Server cannot change its collection internally. To retrieve your original collection name, there are 3 options:

- Check the Windows registry on HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Terminal Server\CentralPublishedResources\PublishedFarms\<CollectionName>
- Check following folder: C:\Windows\RemotePackages\CPubFarms\<CollectionName>
- Download an RDP file via RDWeb and open it in Wordpad. One of the lines is: loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.<CollectionName>

Category Management

Categories are logical groups of applications available to end-users. These categories are visible to end-users in the left pane of the Applications tab in the Awingu application. There are three types of categories:

- Category **All**: The category 'All' contains all applications to which the end-user is authorized. This category is always present and cannot be configured, i.e. this category is not visible in the configuration management console.
- Category **Favorite**: When a user first logs on to Awingu, this category is empty. End-users can add/remove applications to the 'Favorite' category. The category 'Favorite' is always visible to end-users in the user interface, even when it is empty. The category 'Favorite' is built-in to the Awingu application and is not configurable by administrators.
- **Other categories**: System administrators can define additional categories for end-users. These additional categories will be visible to end-users when they are authorized to at least one application that belongs to that category. There is a many-to-many relationship between applications and categories. Administrators can assign zero, one or multiple categories to an application, see Application Management. Similarly, a category can be assigned to zero, one or more applications.

This page provides you the list of existing categories and allows you to add, remove or modify categories.

Drive Management

Introductions

Awingu provides the user with access to file server backends: CIFS, WebDAV and OneDrive for Business. Browsing files is implemented as a series of REST API calls towards the Awingu platform infrastructure. The Awingu platform infrastructure then proxies these REST API calls to another protocol that is supported by the drive back-end. Also creating, renaming, moving, copying, uploading and downloading files is possible. Files can also be opened with configured streamed applications (except when using OneDrive): in this case, the application server will mount the user's drive and open the application with the specified file.

Supported protocols

The current release of Awingu supports the following protocols:

- CIFS with support for:
  - SMB2 and SMB3 (basic) for Windows Server 2008 R2, 2012 R2, 2016 and 2019
  - Samba3 server
- WebDAV with support for:
  - IIS for Windows Server 2008 R2, 2012 R2, 2016 and 2019 with a minimum requirement of WebDAV class 2.
- Microsoft OneDrive for Business (see link for step-by-step instructions to set-up). Note that for OneDrive backends, the user cannot select "Open with" with a streamed application.

From an end-user perspective, there is no noticeable difference in behavior between the different types of back-ends: the same file navigation rules apply to both. It is also possible to move/copy files and directories across file storage back-ends.

It is technically possible to create 2 different drives mapping to the same backend, e.g.:

- Drive "Shared folder" maps to smb://file-server.company.com/Shared/
- Drive "Project folder" maps to smb://file-server/company.com/Shared/Sales/Common/Projects/

In this peculiar case, when an end-user **moves** via the Awingu interface a file/folder from "Shared folder > Sales > Common > Projects" to "Project folder", Awingu does not take into account this maps on the same folder. The Awingu interface will ask whether to overwrite the moved file/folder, resulting in the file/folder to be deleted (because a move, is a copy-overwrite followed with a delete of the original file).

Notes:

- SMB 3.0 Transparent Failover is not yet supported.
- Limited support for Distributed File System (DFS).

Adding/editing drives

Drives are configured to allow end-users accessing file servers via a web-based file manager. Authorization to drives is done in a similar way as configuring authorization to applications, by means of labels.

- **Name**: Name of the drive as it will be displayed in the Awingu end-user interface, in the left pane of the Files tab.
- **Description**: Free text description of the drive.
- **Backend**: Protocol via which the Awingu API will communicate with the file server back-end. Supported protocols:
  - CIFS: also called SMB or Samba
  - WebDAV
  - Microsoft OneDrive For Business. More details here.
- **Client ID**: (only for OneDrive) Client ID (Application ID) of your configured OneDrive Awingu app in Azure.
- **Client secret**: (only for OneDrive) secret created when adding your OneDrive Awingu app to Azure
- **Workspace URL**: (only for OneDrive) the URL a user uses to access Awingu, e.g. https://awingu.mycompany.com
- **Redirect URL**: (only for OneDrive) (read/only) URL to use to configure your OneDrive Awingu app in Azure.
- **URL**: URL of the file server that will be used by the Awingu API to communicate with the fileserver.
  Note that this URL can be parameterized with:
  - **<username>**: the user's username
  - **<domain>**: the name of the domain the user is part of

  URL needs to be based on FQDN name, not NetBIOS.
  Examples:
  - SMB: `smb://file-server.stack.awingu.com/home/<username>/Documents`
  - WEBDAV: `http://file-server.stack.awingu.com:8080/home/<username>/Documents`
  - OneDrive: link to your sharepoint.com environment: `https://mycompany.sharepoint.com`
- **UNC**: UNC that will be used by the application server to access the drives. This UNC path is needed when using "Open with" as action on the Files tab in Awingu.
  Note that this URL can be parameterized with:
  - **<username>**: the user's username

    - **<domain>**: the NETBIOS name of the domain the user is part of
      Example:

      ```
      \\file-server\Home\<username>\Documents
      ```

      UNC needs to be based on netbios name, not FQDN.

  If no UNC path is provided, you can only "Open with" preview (if available).
- **Domain Use**: (only for WebDAV) During authentication against the WebDAV file server, it may be required to pass the domain name. This depends on the configuration of the WebDAV file server. If required, check the box **Use Domain** in Awingu. This option is ignored in case of a CIFS file server back-end.
- **Authentication Role:** (only for CIFS) Defines how to authenticate with the CIFS server
    - User: authenticate as the user accessing the drive
    - Anonymous: authenticate as an anonymous user (should be enabled on the CIFS server)
- **Labels**: Assign labels to drives to create groups of drives. These groups can be used to select, filter, and report on drives.
- **User Labels**: By assigning user labels to drives, you can grant groups of users access to drives. Only users in user groups assigned to a label will see the drive in the Files tab (use *all*: to be visible for all users). For more information on labels, please consult the section Label Management.
- **Context Policy Labels:** Restrict this drive to only be accessible within the provided security context. The context can be configured using the mfa, network or country (2 char ISO 3166-1 alpha code) context policies labels. For network and country, you can define multiple options by using comma separated values. When adding multiple policies, they must all be valid to be able to access the drive. See the *Label Management* page for more information and examples.

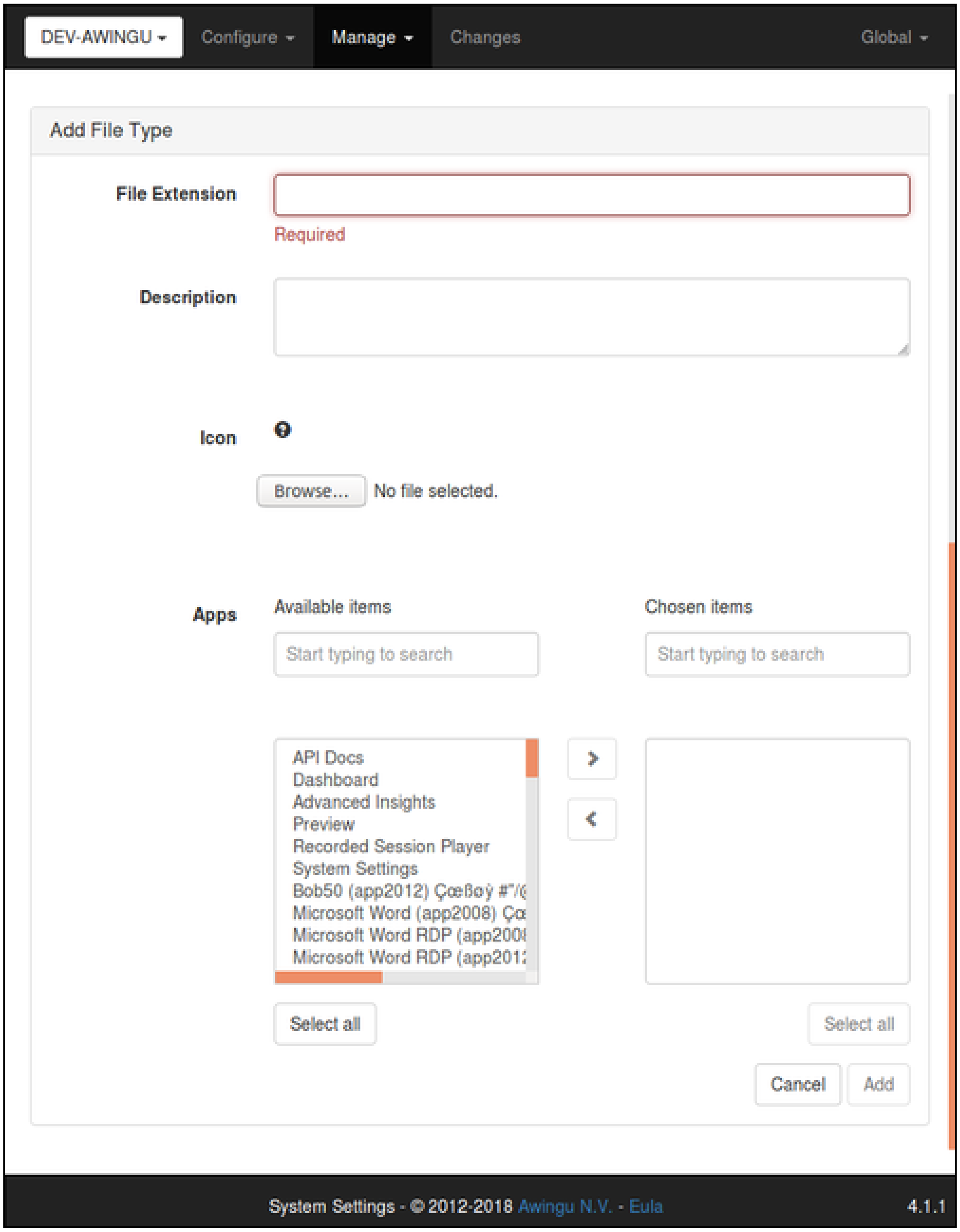
File Type Management

- Introduction
- Linking Application (or preview action) to a file type.

Introduction

File types are the way to link a file on the Awingu Files page to a configured Application. If multiple applications are associated to a file type, the user can choose which one to use.

A selection of common used file types are already configured in Awingu at install time.



Linking Application (or preview action) to a file type.

When opening files in Awingu, the file type of the file is inspected to determine which applications can be used to open the file.

Four parameters are used to define a file type:

- **File Extension**: This is the part of the file name after the leading dot

- **Description**: Free text description
- **Icon**: Icon used to represent the given file type on the Files page in Awingu.
- **Apps**: List of applications that can be used to read or modify this file type

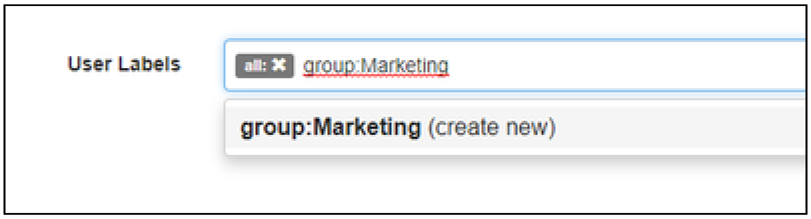
Label Management

Introduction

Labels in Awingu serve different purposes, There are 4 types of labels.

- User Labels: Assign applications, drives or features to users or groups.
- Server Labels: Assign applications to application servers.
- Labels: Attaching a label to applications or drives allows you to use this label when filtering or querying in the *System Settings* or *Dashboard*.
- Context Policy Labels: Define context requirements for applications, drives, features, login or the admin role.

Note: Creating labels can be done on the *Manage > Labels* page of the *System Settings* or it can also be created on the fly when configuring a resource. See example below.



User Labels

User labels are used to assign applications, drives or features to users. Each time a user signs-in, labels are assigned to the user based on their LDAP properties. If you add those labels to application, drives or features, users with the matching labels will have access to this applications or drives, or will have this feature enabled.

> ℹ User Labels need to be created manually or imported (see below). They are not automatically created from the LDAP properties of the logged-in users.

Key	Value	Comments
group	<the name of the security group>*	Custom made user label. Per security group you want to filter on in Awingu, an entry with *group* key needs to be made. You can use *Import groups from AD* to find user groups to auto-generate the labels.
username	<username in DOMAIN\username format>*	Custom made user label. Per user name you want to filter on in Awingu, an entry with *username* key needs to be made. You can use *Import users from AD* to find user groups to auto-generate the labels. ⚠ The domain should be entered in uppercase and username should be entered in lower case, e.g. MYDOMAIN\johndoe
upn	<username in username@fqd-for-upn format>*	Custom made user label. Per user name (via UPN) you want to filter on in Awingu, an entry with *upn* key needs to be made.
ou	<the name of the organizational unit>*	Custom made user label. Per OU you want to filter on in Awingu, an entry with *ou* key needs to be made.
all	(empty)	Predefined user label. Do not remove. When this label is attached to a drive/app/feature, all users from that domain, can access that drive/app/feature.
admin	(empty)	Predefined user label. Do not remove. This label corresponds with the groups indicated as *admin* in the User Connector Configuration.
record	(empty)	Predefined label. Do not remove.

		Add as label to an application (RDP and RemoteApp) to activate session recording (needs to be enabled).
smartcard	(empty)	Predefined label. Do not remove. Add as label to an application (RDP and RemoteApp) to enable Smart Card Redirection.
state	enabled	Predefined user label. Do not remove (system label).

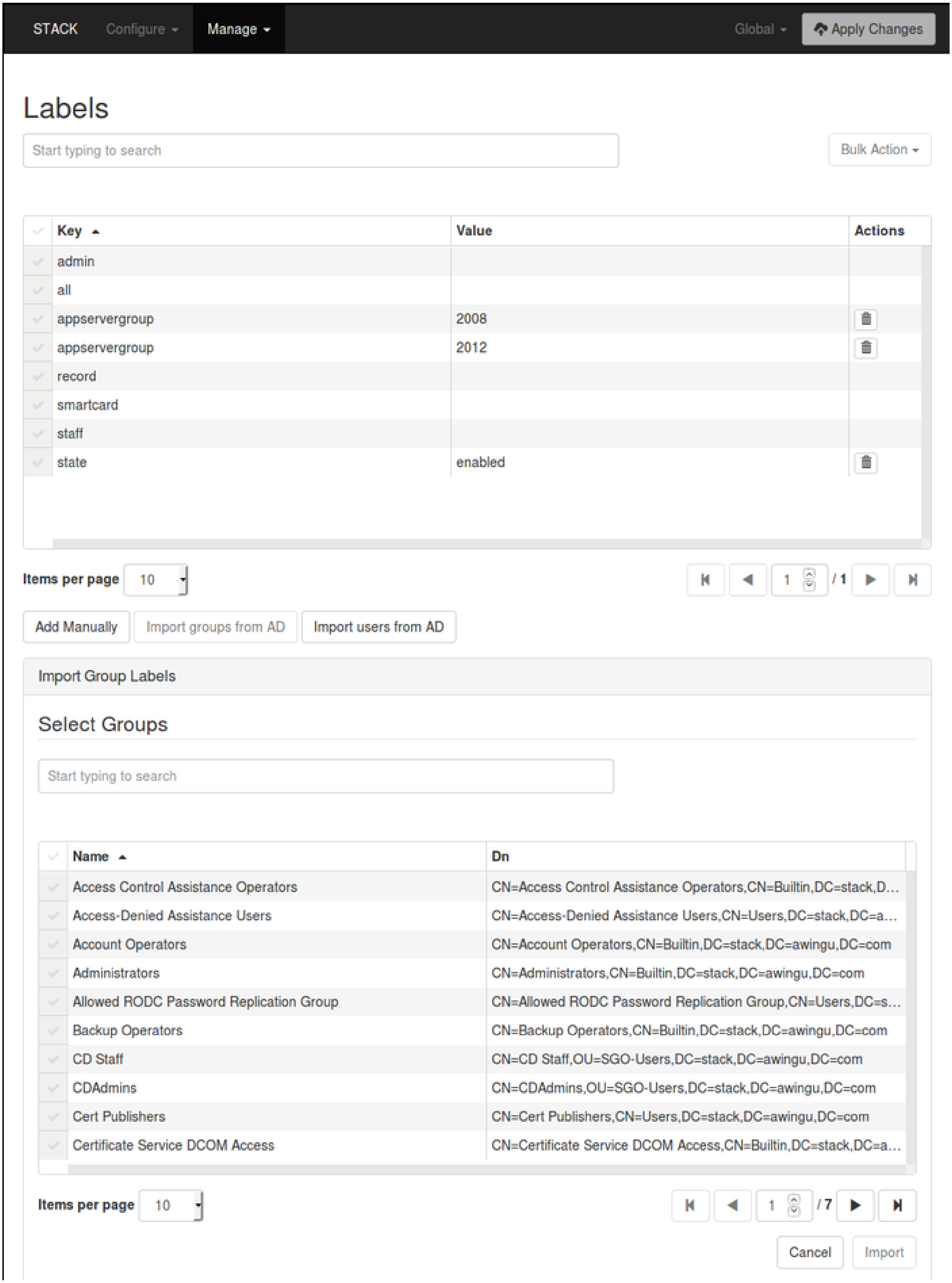
* To look-up the *ou*, *group*, *username* or *upn* of users that have already signed in on Awingu, navigate to Manage > Users: select a user to show the properties, including the labels.

> ⚠ When assigning user labels it needs to be taken into account that the labels are case sensitive.

Importing Labels

To auto-create *group* and *username* labels, you can use the buttons *Import groups from AD* and *Import users from AD*. To be able to use this feature, the bind user needs to be configured in Domain Settings.

When clicking on the button, the groups/users are listed as shown below:



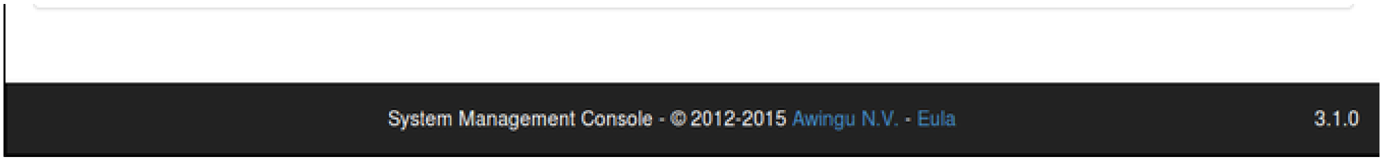
Labels

Key	Value	Actions
admin		
all		
appservergroup	2008	🗑
appservergroup	2012	🗑
record		
smartcard		
staff		
state	enabled	🗑

Import Group Labels

Select Groups

Name	Dn
Access Control Assistance Operators	CN=Access Control Assistance Operators,CN=Builtin,DC=stack,D…
Access-Denied Assistance Users	CN=Access-Denied Assistance Users,CN=Users,DC=stack,DC=a…
Account Operators	CN=Account Operators,CN=Builtin,DC=stack,DC=awingu,DC=com
Administrators	CN=Administrators,CN=Builtin,DC=stack,DC=awingu,DC=com
Allowed RODC Password Replication Group	CN=Allowed RODC Password Replication Group,CN=Users,DC=s…
Backup Operators	CN=Backup Operators,CN=Builtin,DC=stack,DC=awingu,DC=com
CD Staff	CN=CD Staff,OU=SGO-Users,DC=stack,DC=awingu,DC=com
CDAdmins	CN=CDAdmins,OU=SGO-Users,DC=stack,DC=awingu,DC=com
Cert Publishers	CN=Cert Publishers,CN=Users,DC=stack,DC=awingu,DC=com
Certificate Service DCOM Access	CN=Certificate Service DCOM Access,CN=Builtin,DC=stack,DC=a…



System Management Console - © 2012-2015 Awingu N.V. - Eula 3.1.0

You can use the search box to filter. Select the desired groups/users and click on Import.

Example of Use of User Label

We have following AD configuration:

- ou:Europe
  - group:Engineering
  - group:Europe Managers
- ou:America
  - group:Accountancy
  - group:HR
  - group:America Managers
- ou:Global
  - group:Administrators

In User Connector Configuration, we have for this domain:

Domain Administrators	group:Administrators

In Label Management, we have added following rows:

Key	Value
ou	Europe
ou	America
group	Engineering
group	Europe Managers
group	Accountancy
group	HR
group	America Managers

In Drive Management, we have added following user labels to the drives:

Drive	Labels
Home Drive	all:
Engineering Drive	group:Engineering
Accountancy Drive	group:Accountancy
Managers Drive	group:Europe Managers group:America Managers
Administrators Drive	admin:

In Application Management, we have added following User labels to the applications:

Application	Labels
Microsoft Word	all:
AutoCad	group:Engineering
Finance Explorer	group:Accountancy
Cost Calculator	group:Engineering group:Accountancy

Euro Specs	ou:EMEA group:HR
Network Manager	admin:

This results in this overview of rights:

Domain\user and security groups	Available applications	Available drives
John: ou: Europe groups: Engineering, Europe Managers	- Microsoft Word - AutoCad - Cost Calculator - Euro Specs	- Home Drive - Engineering Drive - Managers Drive
Lucy: ou: Europe groups: Engineering	- Microsoft Word - AutoCad - Cost Calculator - Euro Specs	- Home Drive - Engineering Drive
Maria: ou: Europe groups: Administrators	- Dashboard* - System Settings* - Recorded Session Player* - Microsoft Word - Network Manager - Euro Specs	- Home Drive - Administrators Drive
Kim: ou: America groups: Accountancy, America Managers	- Microsoft Word - Finance Explorer - Cost Calculator	- Home Drive - Accountancy Drive - Managers Drive
Patrick: ou: America Groups: HR, America Managers	- Microsoft Word - Euro Specs	- Home Drive - Managers Drive

* pre-installed system application

Server labels

To assign applications to application servers, both the application server and the applications need to have a label in common.

Key	Value	Comments
rdscollection	<the name of the RDS collection>	Custom made server label. See Remote Desktop Service Connection Broker for more information.
<any key>*	<any value>	Custom made server label. Any key* and value can be used to link applications with application servers.

* Any key, except the reserved ones defined in this document.

Labels

All labels can be used for filtering in search boxes and reporting tools. Server and user labels can be used for that purpose, too.

Key	Value	Comments
smartcard	(empty)	Predefined label. Do not remove. See Smart Card Redirection for more information.
audioinput	(empty)	Predefined label. Do not remove, nor use (system label).
<any key>*	<any value>	Custom made label. Any key* and value can be used to filter.

* Any key, except the reserved ones defined in this document.

Context Policy Labels

These labels allow you to define what security context is required to:

- access an application or drive
- use a feature
- login
- be assigned the admin role

We support 3 types of context labels.

- **country**: the value of this label accepts a single or a comma separated list of 2 char ISO 3166-a alpha codes. See https://en.wikipedia.org/wiki/ISO_3166-1 for a full list. E.g. 'country:BE' or 'country:BE,NL'
- **network:** the value of this label accepts both a single IP address (e.g. 'network:172.16.0.15') or a subnet (e.g. 'network:172.16.0.0/8'). Multiple networks or IP addresses can be added using a comma separated list.
- **'mfa:required'**: this label is automatically created. When Multi-Factor Authentication is not required at login, a dialog will be shown explaining the user he will need to re-login and use MFA to access an application, drive or feature,

When combining different types of context labels, they must all be valid before the user has access to the resource,

E.g. The Context Policy Label 'country:BE,NL mfa:required' means that the user will have access to the resource if his IP address comes from Belgium or the Netherlands AND he logged in using Multi-Factor Authentication.

The Awingu System Settings allow administrators to list and filter users. Administrators can also consult more detailed information about a user such as:

- first login date
- last login date
- labels that have been assigned to this user
- email address
- configured locale and keyboard layout

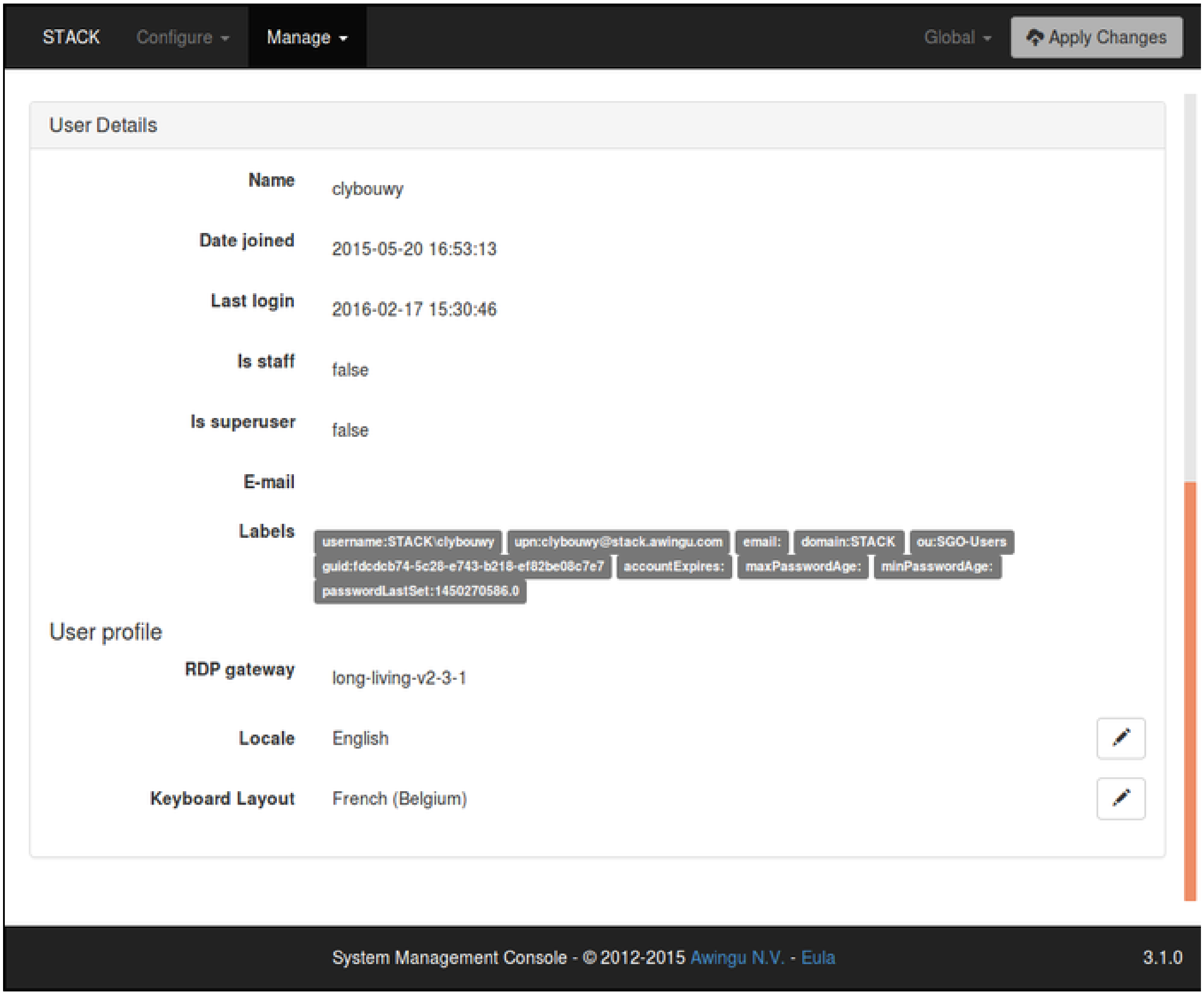
Except for the Keyboard Layout and Locale setting, all parameters are dynamically populated in the database at login into the platform, based on information retrieved from the enterprise authentication infrastructure (AD/LDAP), see also the section User Connector Configuration.

To logout users and close their application session, please refer to Live Monitoring of Users Activity.

Deleting users

Users can be deleted from Awingu, but as long they exists in an authorized user group on the AD/LDAP, they will be able to sign-in again.

Depending on the license type, deleted users will still be shown until the end of the month (the Deleted column will have a checkmark) or they will be deleted immediately.



User Details

Name	clybouwy
Date joined	2015-05-20 16:53:13
Last login	2016-02-17 15:30:46
Is staff	false
Is superuser	false
E-mail	
Labels	username:STACK\clybouwy upn:clybouwy@stack.awingu.com email: domain:STACK ou:SGO-Users guid:fdcdcb74-5c28-e743-b218-ef82be08c7e7 accountExpires: maxPasswordAge: minPasswordAge: passwordLastSet:1450270586.0

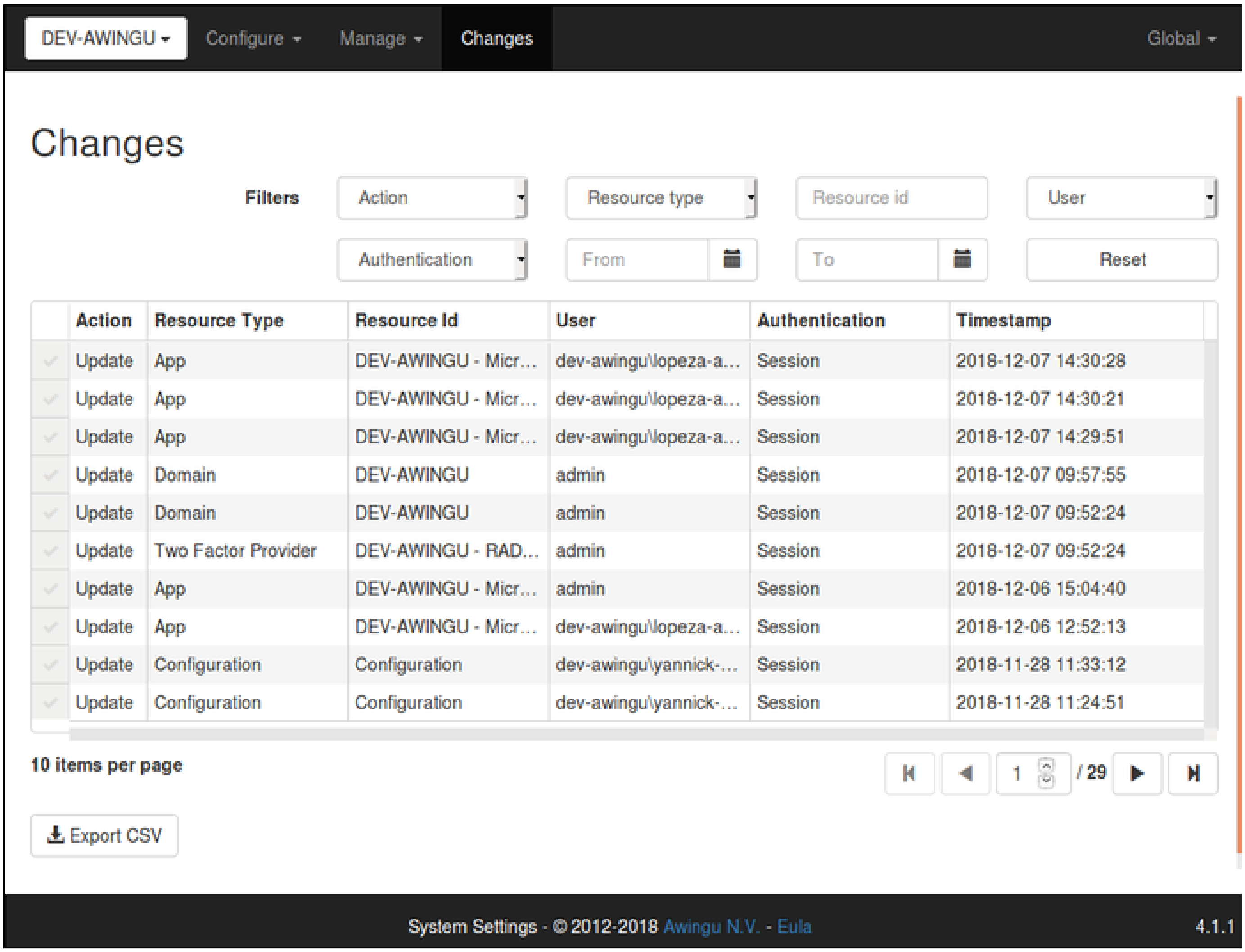
User profile

RDP gateway	long-living-v2-3-1
Locale	English
Keyboard Layout	French (Belgium)

System Management Console - © 2012-2015 Awingu N.V. - Eula 3.1.0

System Settings - Change Log

For auditing reasons, all system settings are logged and kept during 13 months. This applies both for changes done in the System Settings web interface and for changes done through the REST API.



	Action	Resource Type	Resource Id	User	Authentication	Timestamp
✓	Update	App	DEV-AWINGU - Micr...	dev-awingu\lopeza-a...	Session	2018-12-07 14:30:28
✓	Update	App	DEV-AWINGU - Micr...	dev-awingu\lopeza-a...	Session	2018-12-07 14:30:21
✓	Update	App	DEV-AWINGU - Micr...	dev-awingu\lopeza-a...	Session	2018-12-07 14:29:51
✓	Update	Domain	DEV-AWINGU	admin	Session	2018-12-07 09:57:55
✓	Update	Domain	DEV-AWINGU	admin	Session	2018-12-07 09:52:24
✓	Update	Two Factor Provider	DEV-AWINGU - RAD...	admin	Session	2018-12-07 09:52:24
✓	Update	App	DEV-AWINGU - Micr...	admin	Session	2018-12-06 15:04:40
✓	Update	App	DEV-AWINGU - Micr...	dev-awingu\lopeza-a...	Session	2018-12-06 12:52:13
✓	Update	Configuration	Configuration	dev-awingu\yannick-...	Session	2018-11-28 11:33:12
✓	Update	Configuration	Configuration	dev-awingu\yannick-...	Session	2018-11-28 11:24:51

If you are an admin of an administrative domain (global admin) or logged in with the management user (set-up during installation)

- You can select the domain you want to see the changes of with the domain drop-down on the top left
- You can see all global changes, regardless of the selected domain.

If you are a domain admin (non-administrative domain), you will only see changes of your domain. You can export the queried results to a CSV file.

You can filter and list the changes for following fields:

- **Action**: Create / Delete / Update
- **Resource type**: Those are the resources used in the REST API. They mostly map with the corresponding pages of the System Settings.
- **Resource Id**: This is typically the name of the resource, e.g. name of the application, user group, label, etc.
- **User**: User who performed the change.
- **Authentication:** Whether a session (username/password) or API token (see User Connector Configuration) has been used.
- **Timestamp**: Date and time when the change was made.

When clicking on a change in the list, the body of the REST API request and response is shown, even when the change has been done trough the web interface. Example for action *Update*, resource type *Contact*, the change log when editing the phone number of the partner on the General Info page:

- Request:

```
{
    "phoneNumber": "+9876543210"
}
```

- Response:

```
{
    "name": "My Awingu Partner",
    "location": "East-Flandres",
    "uri": "http://172.16.5.65/api/v2/contacts/1/",
    "city": "Gent",
    "phoneNumber": "+9876543210",
    "addressLine1": "Some street 1",
    "country": "Belgium",
    "postalCode": "9000",
    "addressLine2": ""
}
```

Service Provider Support in Awingu

Introduction

Awingu allows service providers to give access to applications and documents to their customers in a secure way.

We will describe 5 possible use cases:

	Number of Awingu environments	Number of Awingu domains	Number of Windows domains	Branding per customer
1	One	One	One	✗
2	One	Multiple (one per customer)	One	✓
3	One	Multiple (one per customer)	Multiple (one per customer)	✓
4	Multiple (one per customer)	One per Awingu	One	✓
5	Multiple (one per customer)	One per Awingu	Multiple (one per customer)	✓

A service provider can combine those use cases, e.g. 1 Awingu environment for multiple small customers and multiple Awingu environments for some of the bigger clients.

For automatic configuration, Awingu offers an API (see Automate Awingu via the REST API).

When using a multi node high available deployment, we strongly recommend to do the SSL offloading at the load balancer.

Case 1: One Awingu / One Awingu Domain / One Windows Domain

Architecture

Access to Awingu:

- All customers access Awingu via the same URL, e.g. https://www.provider.com
- All customers will see the same branding.

For the Awingu topology, following is required

- Multi node setup (for +100 concurrent users)
- External load balancing (for high availability or +200 concurrent users)
- External database (for high availability or +200 concurrent users)

The Windows architecture:

- Only 1 domain with one or multiple domain controllers, file servers and application servers.

- The users of a customer are grouped in the same organizational unit (OU) or security group.

Licensing

Only 1 Awingu license is needed for the desired number of maximum concurrent users.

Configuration

- System Settings > Global > Domain:
    - Define 1 domain.
    - This domain should be an *Administrative domain*.
    - Provide a bind user to allow import.
- System Settings > Configure > User Connector:
    - Define the group(s) that need administrator rights
    - Assign the *Admin* user group label to it
- System Settings > Manage > Labels:
    - In case customers are grouped per OU: create a label per customer:
        - Key: *ou*
        - Value: the name of the OU (case sensitive)
    - In case customers are grouped per security group: use *Import groups from AD*
- System Settings > Manage > Application Servers: define or import the application servers for that domain.
- System Settings > Manage > Applications: define the applications and limit the usage per customer with the ou/group labels.
- System Settings > Manage > Drives: define the drives and limit the usage per customer with the ou/group labels.
- System Settings > Configure > Features: you can limit some features per customer with the ou/group labels.
- System Settings > Configure > Branding: you can only define one branding.

Administration

Only the service provider will be able to manage Awingu. There is no multi tenancy in this case.

Case 2: One Awingu / Multiple Awingu Domains / One Windows Domain

Architecture

Access to Awingu:

- You can define multiple DNS entries pointing to Awingu in order to give each customer his own URL, e.g. https://customer1.provider.com. If you access Awingu via an unknown host header (or via IP address), you can enter your domain manually (if not provided, the default domain will be used).
- You can define branding for each customer.

For the Awingu topology, following is required

- Multi node setup (for +100 concurrent users)
- External load balancing (for high availability or +200 concurrent users)
- External database (for high availability or +200 concurrent users)

The Windows architecture:

- Only 1 domain with one or multiple domain controllers, file servers and application servers.
- The users of a customer are grouped in the same organizational unit (OU) or security group.

Licensing

Only 1 Awingu license is needed for the desired number of maximum concurrent users. You can limit the number of concurrent user per domain.

Configuration

- System Settings > Global > Domain:
    - Define a domain for the employees of the service provider. That domain should be an *Administrative Domain* and should be the *Default* domain.
    - Define 1 domain per customer. Those domains should **not** be *Administrative Domains*. The *NetBIOS Name* is the same for each customer, but the *Name* is different.
    - Per customer domain: provide the Host Header, e.g. customer1.provider.com
    - Per customer domain: provide a bind user to allow import.
    - Per customer domain: define the maximum concurrent users, if desired.

        - In case customers (or the employees of the service provider) are grouped per OU: limit access via the *Base DN*, e.g. "ou=Customer 1,dc=provider,dc=com"
- Per Domain (select via top left):
    - System Settings > Configure > User Connector:
        - User Groups:
            - In case customers (or the employees of the service provider) are grouped per security group:
                - Enable *Sign in White List.*
                - Define the group that should have access and cross the check box *Sign In Whitelist*.
            - Define the group that need administrator rights (and cross the *Sign In Whitelist* check box if applicable):
                - For the domain of the service provider: members of that group can manage all domains and the global settings. We call them Global Admins.
                - For the domain of a customer: members of that group can manage the domain (applications servers, applications, drives, features, branding, etc). As all customers share the same Windows domain, it is not recommended to allow customers themselves to manage their domain. It make more sense that the assigned solution engineer(s) of the service provider are managing the domain. We call them Domain Admins.
        - User Group Labels:
            - Assign the *Admin* label to the defined administrator group
    - System Settings > Manage > Application Servers: define or import the application servers for that domain.
    - System Settings > Manage > Applications: define the applications for that domain.
    - System Settings > Manage > Drives: define the drives for that domain.
    - System Settings > Configure > Features: you can limit some features for that domain.
    - System Settings > Configure > Branding: you can define the branding for that domain.

Administration

Global Admins:

- Are the members of the Admin group defined for the domain for the service provider.
- Can manage all domains and global settings.

Domain Admins:

- Are the members of the Admin group defined for a customer domain.
- Can only manage applications, drives, features, branding etc. of that customer.

The Dashboard is only available for Global Admins.

Case 3: One Awingu / Multiple Awingu Domains / Multiple Windows Domain

Architecture

Access to Awingu:

- You can define multiple DNS entries pointing to Awingu in order to give each customer his own URL, e.g. https://customer1.provider.com. If you access Awingu via an unknown host header (or via IP address), you can enter your domain manually (if not provided, the default domain will be used).
- You can define branding for each customer.

For the Awingu topology, following is required

- Multi node setup (for +100 concurrent users)
- External load balancing (for high availability or +200 concurrent users)
- External database (for high availability or +200 concurrent users)

The Windows architecture:

- Each customer has his own domain with one or multiple domain controllers, file servers and application servers.
- The employees of the service provider will typically have their own domain, too.

Licensing

Only 1 Awingu license is needed for the desired number of maximum concurrent users. You can limit the number of concurrent user per domain.

Configuration

- System Settings > Global > Domain:
    - Define a domain for the employees of the service provider. That domain should be an *Administrative Domain* and should be the *Default* domain.

    - Define 1 domain per customer. Those domains should **not** be *Administrative Domains*. The *NetBIOS Name* will be typically equal to the *Name* of the domain.
    - Per customer domain: provide the Host Header, e.g. customer1.provider.com
    - Per customer domain: provide a bind user to allow import.
    - Per customer domain: define the maximum concurrent users, if desired.
- Per Domain (select via top left):
    - System Settings > Configure > User Connector:
        - User Groups: define the group that need administrator rights:
            - For the domain of the service provider: members of that group can manage all domains and the global settings. We call them Global Admins.
            - For the domain of a customer: members of that group can manage the domain (applications servers, applications, drives, features, branding, etc). Typically, members of that domain are the IT administrators of the customers and/or the solution engineer(s) of the service provider. We call them Domain Admins.
        - User Group Labels:
            - Assign the *Admin* label to the defined administrator group
    - System Settings > Manage > Application Servers: define or import the application servers for that domain.
    - System Settings > Manage > Applications: define the applications for that domain.
    - System Settings > Manage > Drives: define the drives for that domain.
    - System Settings > Configure > Features: you can limit some features for that domain.
    - System Settings > Configure > Branding: you can define the branding for that domain.

Administration

Global Admins:

- Are the members of the Admin group defined for the domain for the service provider.
- Can manage all domains and global settings.

Domain Admins:

- Are the members of the Admin group defined for a customer domain.
- Can only manage applications, drives, features, branding etc. of that customer.

The Dashboard is only available for Global Admins.

Case 4: Multiple Awingus / One Awingu Domain per Awingu / One Windows Domain

Architecture

Access to Awingu:

- Each Awingu environment has its own IP address and DNS entry. Each customer has his own URL, e.g. https://customer1.provider.com.
- You can define branding for each Awingu.

For the Awingu topology, following is required

- Multi node setup for each customer with +100 concurrent users.
- External load balancing for each customer requiring high availability or +200 concurrent users.
- External database for each customer requiring high availability or +200 concurrent users. The same database server(s) can be shared for multiple customers.

The Windows architecture:

- Only 1 domain with one or multiple domain controllers, file servers and application servers.
- The users of a customer are grouped in the same organizational unit (OU) or security group.

Licensing

You need an Awingu license for each Awingu (customer), each one for the desired number of maximum concurrent users.

Configuration

- Per Awingu environment:
    - System Settings > Global > Domain:
        - Define 1 domain.
        - This domain should be an *Administrative domain*.
        - Provide a bind user to allow import.
        - In case customers are grouped per OU: limit access via the *Base DN*, e.g. "ou=Customer 1,dc=provider,dc=com"
    - System Settings > Configure > User Connector:

        - User Groups:
            - In case customers are grouped per security group:
                - Enable *Sign in White List.*
                - Define the group that should have access and cross the check box *Sign In Whitelist*.
            - Define the group that need administrator rights (and cross the *Sign In Whitelist* check box if applicable): members of that group can manage that Awingu environment. As all customers share the same Windows domain, it is not recommended to allow customers themselves to manage their Awingu environment. It make more sense that the assigned solution engineer(s) of the service provider are managing the Awingu environment.
        - User Group Labels:
            - Assign the *Admin* label to the defined administrator group
    - System Settings > Manage > Application Servers: define or import the application servers for that Awingu environment.
    - System Settings > Manage > Applications: define the applications for that Awingu environment.
    - System Settings > Manage > Drives: define the drives for that Awingu environment.
    - System Settings > Configure > Features: you can limit some features for that Awingu environment.
    - System Settings > Configure > Branding: you can define the branding for that Awingu environment.

Administration

Each Awingu environment can be fully managed by the members of the Admin group defined for each environment.

Case 5: Multiple Awingus / One Awingu Domain per Awingu / Multiple Windows Domains

Architecture

Access to Awingu:

- Each Awingu environment has its own IP address and DNS entry. Each customer has his own URL, e.g. https://customer1.provider.com.
- You can define branding for each Awingu.

For the Awingu topology, following is required

- Multi node setup for each customer with +100 concurrent users.
- External load balancing for each customer requiring high availability or +200 concurrent users.
- External database for each customer requiring high availability or +200 concurrent users. The same database server(s) can be shared for multiple customers.

The Windows architecture:

- Each customer has his own domain with one or multiple domain controllers, file servers and application servers.

Licensing

You need an Awingu license for each Awingu (customer), each one for the desired number of maximum concurrent users.

Configuration

- Per Awingu environment:
    - System Settings > Global > Domain:
        - Define 1 domain.
        - This domain should be an *Administrative domain*.
        - Provide a bind user to allow import.
    - System Settings > Configure > User Connector:
        - User Groups: define the group that need administrator rights. Members of that group can manage that Awingu environment. Typically, members of that domain are the IT administrators of the customers and/or the solution engineer (s) of the service provider.
        - User Group Labels: assign the *Admin* label to the defined administrator group
    - System Settings > Manage > Application Servers: define or import the application servers for that Awingu environment.
    - System Settings > Manage > Applications: define the applications for that Awingu environment.
    - System Settings > Manage > Drives: define the drives for that Awingu environment.
    - System Settings > Configure > Features: you can limit some features for that Awingu environment.
    - System Settings > Configure > Branding: you can define the branding for that Awingu environment.

Administration

Each Awingu environment can be fully managed by the members of the Admin group defined for each environment.

Monitoring and Reporting

Introduction

The **Dashboard** can be found in Applications. You need to be signed in as a user belonging to a user group labeled as *admin*.

Status Overview of Services on All Servers

The **Status** tab of the Dashboard provides a heath-map of servers (vertical axis) versus components (horizontal axis). This tab is only available for admins of an administrative domain (global admins) and the management user (defined at installation).

The following color code convention is adopted:

- Empty: The corresponding component is not installed on this server.
- Dark gray: The component is installed but no data are available.
- Green: The corresponding component is running on the server.
- Orange: One of the corresponding sub components is installed, but not running on the server
- Red: The corresponding component is installed but not running on the server.

Clicking on a component bubble you to a detailed page with more information on the particular component on that server.
Clicking on a server will lead you to a detailed page with more information on the server.

Monitoring Servers and Components

From the **Servers** tab in the Dashboard, system administrators can obtain more detailed information on servers and processes. This tab is only available for admins of an administrative domain (global admins) and the management user (defined at installation).

On the servers tab a list of servers is presented, together with hostname and status.
Clicking on a server leads you to a detailed page with statistics and components.

Statistics are shown over a configurable time interval for the following parameters:

- Memory Usage
- CPU Usage
- Status Information (running/halted)
- Disk Usage

All components/processes installed on that server are also shown with the following attributes:

- Name of component
- IP address
- Port
- Status

Clicking on a component leads you to a page with more details on the component.

Awingu License Tracking

Awingu provides system administrators the means to track license consumption, as part of the Dashboard.
The following metrics are shown:

- Number of named users.
- Number of concurrent user sessions. The "Concurrent User Count" field in your Awingu license (see General Information) is the maximum value allowed for this metric.

This tab is only available for admins of an administrative domain (global admins) and the management user (defined at installation).

Number of Named Users

This metric tracks the number of named users on the Awingu platform on a calendar month basis. The graph shows the number of named users for the past 12 months as well as for the current month.

All named users know to Awingu (list visible on the System Settings > Manage > Users page) for a given month will count towards this metric even the user did not login to Awingu.

The graph and metric is not updated real-time, but twice a day.

Deleting Users

Users can be deleted on the System Settings > Manage > Users page. Depending on the license type, deleted users will still be shown and counted towards the named users metric until the end of the month (the Deleted column will have a checkmark) or they will be deleted immediately.

For users that have been removed from Awingu (System Settings > Manage > Users), an entry will be re-created at next login time.

Peak Number of Concurrent User Sessions

This metric tracks the peak number of browsers signed-in to Awingu on a calendar month basis. It shows the number of concurrent user sessions for the past 12 months as well as for the current month. For the current calendar month, the value is peak number of concurrent sessions up to the current date.

The "Concurrent User Count" field in your Awingu license (see General Information) is the maximum value allowed for this metric. The management user, created during installation, does not count as concurrent user.

Note that the values are not updated real-time, but every 5 minutes.

Example

Please follow this example on how the data for the license graphs are generated:

Time stamp	Action	Named Users	Concurrent User Sessions
2019-01-01 09:00	Awingu is just installed	0	0
2019-01-01 10:00	Ada signs-in and opens the streamed app Word	1	1
2019-01-01 10:01	Youssef signs-in and opens the streamed apps Word and Excel	2	2
2019-01-01 10:03	Ada signs-out without closing Word (app is disconnected)	2	1
2019-01-01 10:04	Ada signs-in on other device and recovers the Word app	2	2
2019-01-01 10:05	Youssef closes Word and Excel and signs-out	2	1
2019-01-01 10:06	Ada closes Word and signs-out	2	0
2019-01-01 10:07	Wong signs-in	3	1
2019-01-01 10:08	Wong signs-out	3	0
January 2019	**Resulting graphs (peak)**	**3**	**2**

Live Monitoring of Users Activity

The **Activity** page in the Dashboard gives administrators insights in the current usage of the platform and allows them to logout users, terminate and view their application sessions.

More specifically, it gives information regarding the number of simultaneous connected browsers to the platform, a.k.a. the number of concurrent users.

Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

- **Total active concurrent user sessions**: counts the number of currently connected concurrent users.
- **Total disconnected user sessions**: counts the number of user sessions that have not been properly closed. This can happen when a user closes the browser without logging out of Awingu or when the battery of the end-user device fails, or when the end-user experiences a connectivity glitch. In those cases, the sessions remain the **disconnected** state for 10 up to 15 minutes. The list is refreshed at a 5 minute interval.

The table below provides more details regarding the individually connected users:

- Each row represents a user session.
- Per user session, it is possible to see the session ID, the start time of the session, the disconnect time of the session (if applicable), the country and the current status.
- Each user session can be individually logged out.
- Per user session, the linked application sessions can be shown by clicking the view details button (+ icon) on the left.
- Per application session, it is possible to see the application session ID, the application name, the start and end time, the used application server, whether the session was recorded and the status.
- Following actions can be done on an application session:
    - View session (eye icon): A new browser tab will be opened and after the user of the application session accepted the join request, the admin will be able to view the application session. The admin can also ask keyboard and mouse control of the application session and provide support if necessary.
    - Terminate: The application session will be forcefully terminated and all unsaved changes will be lost.

Note that the countries shown in the table are based on a static geo IP database defined during installation or the last upgrade. Those locations might not be accurate anymore.

Monitoring the Application Connector

From the **Application Overview** tab in the Dashboard, system administrators can obtain information about applications and application servers.

Admins of an administrative domain (global admins) and the management user (defined at installation) can filter the views for specific domains with the dropdown on the top left. Domain admins only see content of their domain.

Application Servers

For each server, one can see the number

- active sessions: active applications streamed to the end users
- reserved sessions: a session is reserved when a user requests to open a streamed application. When the application is actually started, the session is not *reserved* anymore, but *active*.

Note that the sum of the active and reserved sessions cannot be higher than *Max Connections* defined for that application server.

Applications

For each streamed application, one can click through the application insights, showing the number of unique users that used the application (monthly), the maximum concurrent usage of the application (monthly) and how many time each user has used the application. The data can be filtered with the date picker on the top.

Insights Reporting

The Insights tab contains some overall information about the usage of Awingu. Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

Application Usage

The table shows the number of distinct named users that have been using a particular streamed application over a configurable time interval.

OS and Browser

This page provides 2 tables that show information about the **end-user device OS** and **browser usage** over a configurable time interval. Every browser session is counted. So for example, if a user has signed-in 20 times during the specified time interval, this will count as 20 sessions in both pie charts.

Audit Reporting

The Audit reporting tab in the Dashboard provides system administrators further insights in the usage of the Awingu system. Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

All data is kept for 13 months. The output can be exported to CSV.

Note: The date/time is shown in UTC.

Query Syntax

On each page, the admin can query and/or change the date period to limit the shown output.

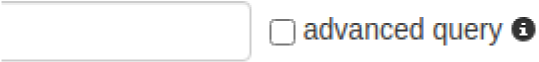
Examples of query strings:

Query	Expected result
john	All records containing the full word "john"
john*	All records containing a word starting with "john"
john	All records containing "john" anywhere
john alice	All records containing the full words "john" or "alice"
john AND alice	All records containing the full words "john" and "alice"
NOT john	All records not containing the full word "john"
@timestamp:{2018-05-02T19:00 TO 2018-05-02T20:00}	All records with timestamp between given times

Advanced Querying

Using *advanced query* you can use a DSL (Domain Specific Language) to perform more fine-grained filtering.

To enable advanced querying, make sure you tick the ‘advanced query' box on the right-hand side of the filter input:



The field names to use in a query are different from the column names in the view. To get an overview of the field names available for the current view, click on the `i` icon next to *advanced query.*

Below an example of view specific information for *Shared Application Session Settings* audit logs

How to use advanced query filtering

Filtering

The basic filter syntax for a comparison of a field to a value is as follow

```
[field] ([negation]) [filter operator] [value]
```

The `field` is the name of field to be queried. The `value` is the value the field shall be compared to. Values for strings and timestamps need to be quoted in single quotes. For boolean fields the values `true` and `false` are valid.

The possible values for the `filter operator` are listed in the table further below. Some of these filters can be negated with the optional keyword `not`, to see which operators support negation also see the table below.

Filter operator	Alias	Meaning	Negatable with "not"	Field type requirements

`=`	`eq`	"equal to"	= is not, but the eq alias is negatable	-
`!=`	`not eq`	"not equal to"	no	-
`<`	`lt`	"less than"	no	-
`>`	`gt`	"greater than"	no	-
`<=`	`lte`	"less than or equal to"	no	-
`>=`	`gte`	"greater than or equal to"	no	-
`contains`		substring search (case sensitive)	yes	requires text or char fields
`icontains`		substring search (case insensitive)	yes	requires text or char fields
`startswith`		substring search at the beginning of the field value (case sensitive)	yes	requires text or char fields
`istartswith`		substring search at the beginning of the field value (case insensitive)	yes	requires text or char fields
`endswith`		substring search at the end of the field value (case sensitive)	yes	requires text or char fields
`iendswith`		substring search at the end of the field value (case insensitive)	yes	requires text or char fields
`isnull`		value must be NULL	yes	-

User Sessions

The user sessions show a list of sessions with following information:

Property	Meaning
Start	The start date/time of the Awingu session (when logging on to Awingu)
End	The end date/time of the Awingu session (at disconnect or at logout)
Domain	The Awingu domain of the user
User Session Id	The internal user session id, which can be used to filter on the other audit pages.
Ip	The IP address of the machine which started the Awingu session
Username	The domain\username
Mfa	Wether Multi-Factor Authentication was used or not when logging in.
Latitude	Latitude coordinate/ based on geo IP (which is indicative).
Longitude	Longitude coordinate/ based on geo IP (which is indicative).
Labels	All (user) labels fetched from the AD/LDAP

Application Sessions

This only applies for streamed applications (RDP and RemoteApp).

Property	Meaning
Start	The start date/time of an application session
End	The end date/time of an application session
Domain	The Awingu domain of the user opening the application

Client Session Id	The internal id for the connection between browser and Awingu*
Application Session Id	The internal id for the connection between Awingu and application servers
User Session Id	The User session id (cf. User Sessions)
Client Session Numeric Id	Short version of the Client Session Id*
Application Key	The internal Awingu id for application (cf. Application Overview > Applications)
Server	The DNS or IP address of the application server
Port	The server port used to connect to the application server
Exe	The alias of the RemoteApp (empty for RDP applications)
Recorded	Whether the application sessions has been recorded.

* This id changes at each time the session is taken over on another device or in another browser tab.

Correlate with the logs on the application server

If you want to correlate an application session in Awingu with an RDP session on application server, for that application session, you need to find the oldest log entry. The Client Session Numeric Id corresponding to that entry is the one used at startup of that application session.

This Client Session Numeric Id can be found on the application server **during the connection**:

- Windows Task Manager:
  On the Users tab, the column "Client name" (not shown by default) contains the Client Session Numeric Id (prefixed with AW-)
- Server Manager (Windows 2008 only):
  In left column go to Roles > Remote Desktop Services > Remote Desktop Services Manager.
  - Users tab: right-click and click on Status. The "Client name" contains the Client Session Numeric Id and the "Client address" contains the real IP address of the user.
  - Sessions tab: the column "ClientName." contains the Client Session Numeric Id.

This Client Session Numeric Id can be found on the application server **post mortem**:

- In the Event Viewer, go to Windows Logs > Security. Click on "Find..." in the right column to search for the Client Session Numeric Id (prefixed with "AW-").
  The event has following properties:
  - Keywords: Audit Success
  - Source: Microsoft Windows security auditing
  - Task Category: Logon

Shared Application Sessions

The Shared Application Sessions view lists all guests that joined a shared application session.

Property	Meaning
Start	Timestamp on which the client joined the shared application session
End	Timestamp on which the client joined the shared application session
Client Session Id	The internal id for the connection between browser (guest) and Awingu
Client Session Numeric Id	The internal id for the connection between browser (host) and Awingu (is equal to the Client Session Numeric Id of the host of the application session)
IP	The IP address of the client that joined the shared application session

* Is equal to the Client Session Numeric Id of the host of the application session

Share Application Sessions Settings

The Shared Application Sessions Settings view lists all shared application sessions and their settings (changes).

Property	Meaning
Timestamp	The timestamp on which the settings where applied

Domain	The Awingu domain of the user opening the application
Client Session Id	The internal id for the connection between browser (guest) and Awingu
Application Session Id	The internal id for the connection between Awingu and application servers
User Session Id	The User session id (cf. User Sessions)
Joinable	Can users join the session
Is Protected	Is a password required to join the session
Join Mode	How is the session shared (`SINGLE` or `MULTI`)
Access Rights	How are access rights determined? (`PUBLIC`, `DOMAIN` or `USER`)

Web Applications

The Web Applications view lists all web applications accessed through Awingu:

- For all web applications, each time a user clicks on the application within Awingu, this is logged.
- For a reverse proxied web application, we also log when the user browses directly to the configured source host header, but the session cookie is not valid anymore. This is the case when the user has logged out from Awingu since the last visit of the web application.

Property	Meaning
Timestamp	Timestamp on which the user has opened the web application
Domain	The Awingu domain of the user opening the web application
User Session Id	The User session id (cf. User Sessions)
Name	Name of the Web Application
Url	Destination URL of the Web Application (connection between Awingu and web server)
Behind Reverse Proxy	Whether the built-in reverse proxy is used for the web application

IdP Sessions

Only applicable if Awingu is configured to be used a Identity Provider for Single Sign-On (SSO)

Property	Meaning
Login Time	Timestamp an external SSO Service requests Awingu to identify a user
Domain	The Awingu domain of the user opening the web application
Service Provider Name	Name of the service provider, as mentioned in User Connector Configuration
Username	The username
User Session Id	The User session id (cf. User Sessions)
Assertion Customer Service	ACS URL, as configured for the SSO service
Request Issuer	Issuer, as configured for the SSO service
Request Id	SAML request ID, provide by the SSO service

Shares

The Shares view lists the creation, update, access and deletion of all shares.

Property	Meaning
Timestamp	Timestamp of the log entry
Domain	The Awingu domain of the user that created the share

User Session Id	For create/update/delete: the User session id (cf. User Sessions) performing the action For access: the User session id (cf. User Sessions) accessing the share*
Ip	IP address of the client that created/updated/deleted/accessed the share
country	Country based on geo IP for the listed IP address
Action	Can be create, update**, access or delete.
Name	Name of the share
Drive	Drive from which the file/folder was shared
Path	File path of the shared file/folder
Content Type	Content type of the share
Created By	Username of the user that shared the file
Expires	Expiration date of the share
Id	Internal ID of the share
Folder	Indicates if the share is a folder
Public	Indicates if the share is publicly accessible
Mode	Mode in which the file was shared (DOWNLOAD or PREVIEW)
Checsum	Checksum of the shared file (when accessed)
Range	Range accessed during request***

* Anonymous access of a public share leads to an empty value.
** A share is updated when a property (e.g. Expiry date/time) has changed or the content has been updated (via Update button in end-user UI).
*** A single access to a shared *preview* document can lead to multiple entries in the list. When viewing the document, this can be downloaded in multiple chuncks into the PDF reader, leading to multiple requests and entries. This allows you to see if a document was downloaded entirely or not.

Files

The Files view lists all file actions using Awingu. Note that in-app file actions can not be audited, because this happens directly between the application server and the file server. Only actions invoked in the Workspace and Files page can be tracked via Awingu.

Property	Meaning
Timestamp	Timestamp of the log entry
Domain	The Awingu domain of the user that performs the file action
User Session Id	The User session id (cf. User Sessions)
Action	The performed file action, e.g. copy, move*, create folder, upload, ...
Drive	The drive where the file is located
File Path	The path where the file is located
Destination Drive	In case of copy or move: the drive where the file has been copied/moved to
Destination File Path	In case of copy or move: the path where the file has been copied/moved to

* Renames are treated as moves, where the destination file path is showing the new name.

Anomaly Reporting

The Anomalies reporting tab in the Dashboard provides system administrators insight in unusual activities on the Awingu environment.

Admins of an administrative domain (global admins) and the management user (defined at installation) can filter for specific domains with the dropdown on the top left. Domain admins only see users of their domain.

The admin can query and/or change the date period to limit the shown output, which can be exported to CSV. The query syntax is the same as for Audit Reporting.

Following anomalies are reported:

Code	Category	Description
COUNTRY_MISMATCH	LOGIN	Same user is logged in in 2 different countries simultaneously
TRAVEL_SPEED	LOGIN	The distance between to logins is too far to travel at realistic speed
TOO_MANY_FAILED_ATTEMPTS	LOGIN	A user uses the wrong password more than 3 times
NEW_BROWSER	LOGIN	A user logs in with a new browser
CONTEXT_RESTRICTION	CONTEXT	A user tried to perform an action that was prohibited due to context restrictions

For each detected anomaly, following information is provided:

Property	Meaning
Timestamp	Timestamp of the detected anomaly (UTC)
Domain	Domain of the user
Category	Only `LOGIN` and `CONTEXT` categories are supported by now
Code	Type of anomaly (see table above)
Description	More details of the actual anomaly
Ip	IP address of the user
Users Session Id	Users Session Id in case the user logged in (see Audit Reporting)
Username	domain\username

Country mismatch anomaly

At each login, we identify the country of the user based on his IP address. If a user is logged in simultaneously in two or more different countries, a COUNTRY_MISMATCH anomaly will be logged. The description field will mention the detected countries.

Travel speed anomaly

At each login, we identify the location of the user based on his IP address. If the distance of a user between the last logout and the current successful login would imply that the user would travel at a speed of more than 1000 km/h, a TRAVEL_SPEED anomaly will be logged. The description field will mention the distance and calculated speed in metric and imperial units.

Too many failed attempts anomaly

When a user fails 3 times consecutively to login, because of a wrong password or a wrong MFA (Multi Factor Authentication) attempt, a TOO_MANY_FAILED_ATTEMPTS anomaly will be logged. The description field will mention the number of consecutive failed attempts.

Note: if a user has never logged in to Awingu before, the anomaly won't be logged.

New browser anomaly

When a user logs in for the first time to Awingu on a certain browser, a fingerprint is calculated to identify the browser. This fingerprint is stored locally in the browser. At each successful login, that fingerprint is sent to Awingu and if the fingerprint is different from the one of the previous successful login, a NEW_BROWSER anomaly is logged. The description field will mention the fingerprint.

To calculate the fingerprint, different parameters are taken into account, like user agent, language, screen resolution, time zone etc. If one of those parameters changes, the fingerprint will not be recalculated as long the previous fingerprint is still stored locally in the browser. If the user however clears the local storage of the browser, the fingerprint will be recalculated and an anomaly will be logged.

Integration

Integrating with existing Windows environment

Introduction

Although there are many possibilities to the Awingu plaform into your existing IT environment, below you can find some useful remarks about this integration effort.

Using the Active Directory Server as NTP server

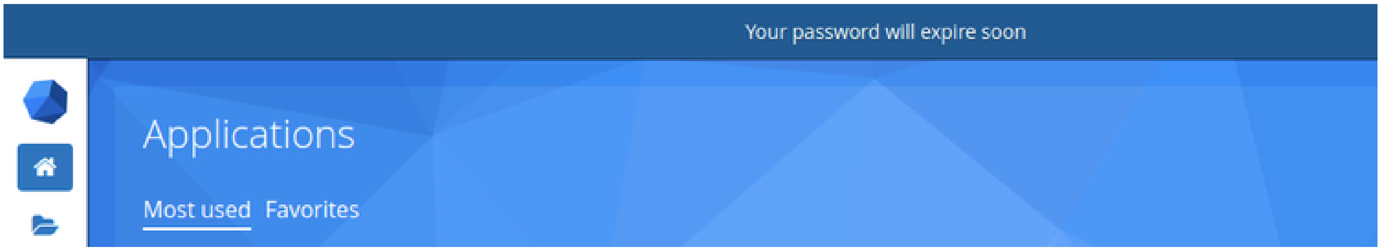
When you configure Awingu to use the time service of your Active Directory Server as NTP server, you need to make sure that the AD server has a reliable time source. The easiest option is to sync your AD server with a public NTP server pool, like nist.gov.

Example for Windows 2012 (can only be done via PowerShell):

```
net stop w32time
w32tm /config /syncfromflags:manual /manualpeerlist:"time-a.nist.gov, time-b.nist.gov, time-c.nist.gov, time-d.nist.gov"
w32tm /config /reliable:yes
net start w32time
```

Password expiry notification

When the password of a user is going to expire in less than 15 days or the last time the password was changed is too long ago, a notification at the top of the workspace is shown (see screenshot below).



The properties we use are:

- msDS-UserPasswordExpiryTimeComputed
- passwordlastset

Organizational Units for users and application servers

Depending on the needs and the set-up of the customer Windows organization, there are multiple ways of organizing the Awingu platform in the windows domain structure.

If users from separate organizational units (OU's) need to connect to the Awingu platform, we believe it is useful to set-up the application servers into a separated OU. Such a set-up allows to straightforward set-up Group Policy rules on the pool of application servers. If the user processing loopback Group Policy Object (GPO) is set within this application server OU, it is possible to apply and override user side policy rules when they are logging into the application servers. This way special user side policy rules can be applied on the application servers for all users logging in the application servers.

To configure the User Group Policy loopback processing mode, create and link a new GPO to your application server OU where the following is set:

- computer Configuration / Policies / Administrative Templates / System / Group Policy / user Group Loopback processing mode: This GPO can be set-up in either merge or replace mode.
  In merge mode, all user side GPOs of the users original OU are first applied, afterwards the GPOs specific to the application server is applied.
  In replace mode, only the user side GPO of the application servers are applied. If you opt for replace mode, all the user that start apps on the application server will experience exactly the same behavior.

Group Policy recommendations

As described above, we recommend adding a few GPOs on the Awingu users and application servers.

GPOs for the Awingu users

Following GPOs are optional:

- User Configuration / Policies / Administrative Templates:
  - Start Menu and Taskbar: Remove Run menu from Start Menu: **Enable**
  - System: Prevent access to the command prompt: **Enable** (Disable the command prompt script processing also? **No**)
  - System: Ctrl+Alt+Delete Options: Remove Task Manager **Enable**
  - System: Ctrl+Alt+Delete Options: Remove Lock Computer **Enable**
  - Windows Components Desktop Window Manager: Do not allow window animation: **Enable**
  - Windows Components / Windows Explorer: Hide these specified drives in My Computer: **Enable** (Pick one of the following combinations: **Restrict all drives.**)
  - Windows Components / Windows Explorer: No Computers Near Me in Network Locations: **Enabled**
  - Windows Components / Windows Explorer: No Entire Network in Network Locations: **Enabled**
  - Windows Components / Windows Explorer: Prevent access to drives from My Computer: **Enabled** (Pick one of the following combinations: **Restrict all drives**)
  - Windows Components / Windows Explorer: Remove "Map Network Drive" and "Disconnect Network Drive": **Enabled**
  - Windows Components / Windows Explorer: Hides the Manage item on the Windows Explorer context menu: **Enabled**
  - Windows Components / Windows Explorer: Remove Hardware tab: **Enabled**
  - Windows Components / Windows Explorer: Remove “Map Network Drive” and “Disconnect Network Drive”: **Enabled**
  - Windows Components / Windows Explorer: Remove Search button from Windows Explorer: **Enabled**
  - Windows Components / Windows Explorer: Disable Windows Explorer's default context menu: **Enabled**
  - Windows Components / Windows Powershell: Turn on script execution: **Enabled** with **Allow only signed scripts**
  - Windows Components / Remote Desktop Services/Remote Desktop Session Host/Session Time Limits: Set time limit for disconnected sessions: **Enable** (End a disconnected session: **1 minute**)
  - Windows Components / Remote Desktop Services/Remote Desktop Session Host/Session Time Limits: Set time limit for log off of RemoteApp sessions: **Enable** (RemoteApp session logoff delay: **1 minute**)

More settings are described in e.g. http://nikoscloud.wordpress.com/2013/04/23/how-to-secure-your-remote-desktop-server-with-gpo/

GPOs for the application servers

- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Session Host / Connections:
    - ⚠ Required: Restrict Remote Desktop Services users to a single Remote Desktop Services sessions: **Disable**.
    - ⚠ Required: Automatic reconnection: **Enable**.
    - ⚠ Needed when you want to publish programs in Awingu as an RDP application: Allow remote start of unlisted programs: **Enable**.
- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Sessions Host / Session Time Limits:
    - ⚠ Required: Set time limit for disconnected sessions: End a disconnected session in **1 minutes**
    - ⚠ Required: Set time limit for log off of RemoteApp sessions: RemoteApp session log off delay **Immediately**
- Computer Configuration / Policies / Administrative Templates / Windows Components / Remote Desktop Services / Remote Desktop Sessions Host / Device and Resource Redirection:
    - ℹ Optional: Allow time zone redirection: **Enable**.

Set-up Drives connectivity

CIFS connectivity:

For Awingu to allow connections to the CIFS backend, the specific servers needs to enable SMB shares and SMB connectivity should be allowed to the Awingu environment (for multi node Awingu setup: connect to workers and frontend nodes).

Please be sure the SMB protocol is enabled on your server. You can use following cmdlet:

```
Set-SmbServerConfiguration -EnableSMB2Protocol $true
```

WebDAV drives:

In order to have access to your webdrive, the file structure needs to be published via Webdav on your file servers. Our WebDAV connector needs at least DAV protocol version 2.

To set-up WebDAV via IIS (version 8)

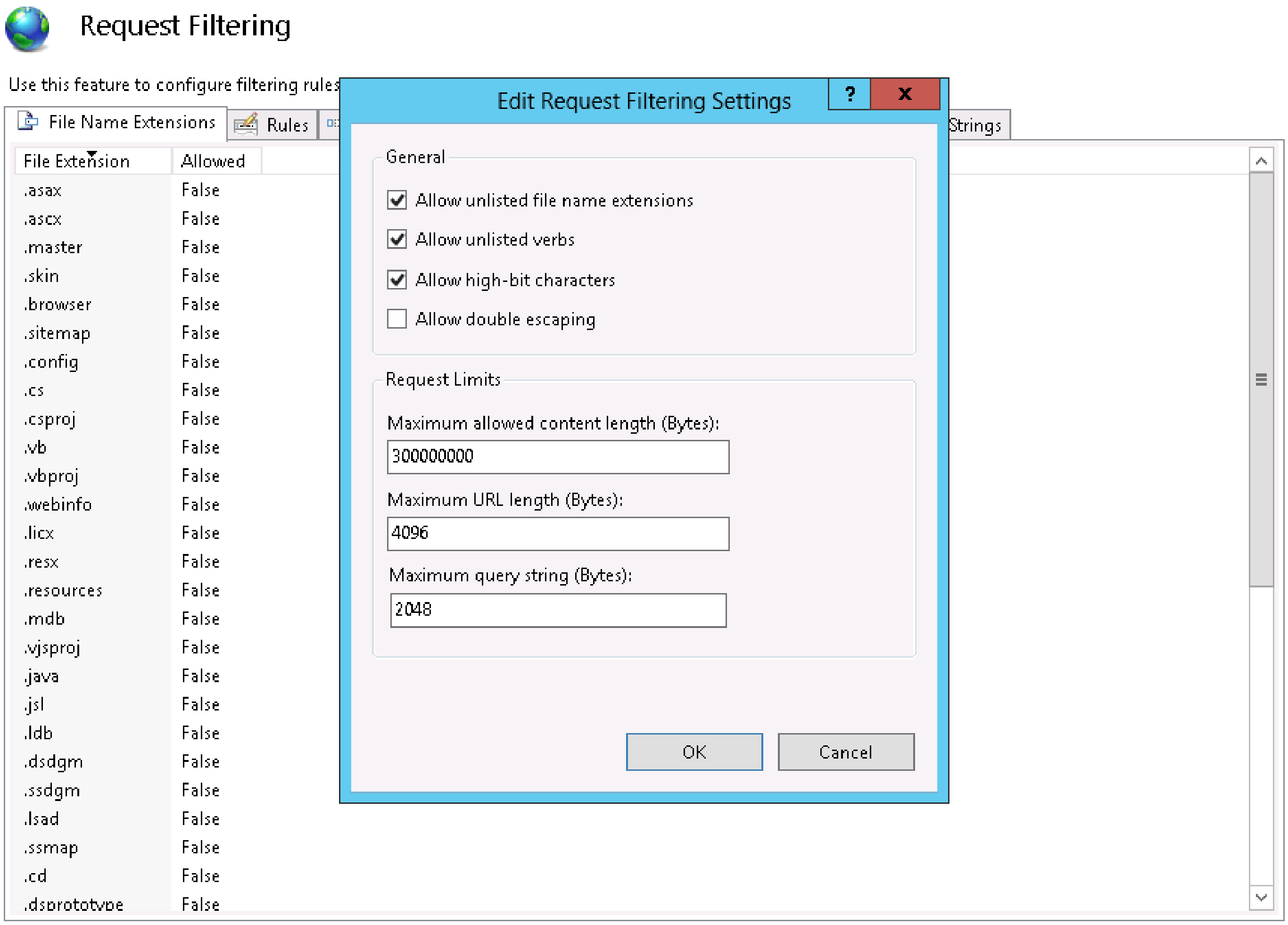
1. Install the IIS server role and features:
    a. Add the IIS role, no extra feature, ignore WSRM,
    b. IIS Features: Common HTTP Features: Webdav Publishing, default document, Directory Browsing, Http Errors, Http Redirection, Static Content.
    c. IIS Features: Health Diagnostics: Custom logging, HTTP logging, Logging Tools
    d. IIS FeatureS: Authentication: Click on everything
2. Go to Manager IIS Manager
    a. Add an application pool called webdav
    b. Rename the Default site
    c. Add a website: webdav connect it to share location
    d. Bind it to port 80
    e. Webdav
        i. Add Authorizing Rule (that all users can connect)
        ii. Enable WebDav
    f. Authentication
        i. Enable Basic, Digest and Windows.

WebDAV support for large files

By default IIS WebDAV has request filtering turned on, which limits the default upload size to 30000000 Bytes, which is approximately 28.6MiB. Refer to this guide to change these settings.

In summary

- Open the IIS Manager:
    - Click on the left pane to your WebDAV site.
    - Find and clink on the middle pane 'Request Filtering'.
    - Edit on the right pane: 'Edit Request Filtering Settings'
    - In this dialog box, you can change the default value of the Maximum Allowed content length (Bytes).



Request Filtering

Use this feature to configure filtering rules

File Extension	Allowed
.asax	False
.ascx	False
.master	False
.skin	False
.browser	False
.sitemap	False
.config	False
.cs	False
.csproj	False
.vb	False
.vbproj	False
.webinfo	False
.licx	False
.resx	False
.resources	False
.mdb	False
.vjsproj	False
.java	False
.jsl	False
.ldb	False
.dsdgm	False
.ssdgm	False
.lsad	False
.ssmap	False
.cd	False
.dsprototype	False

Edit Request Filtering Settings

General

☑ Allow unlisted file name extensions

☑ Allow unlisted verbs

☑ Allow high-bit characters

☐ Allow double escaping

Request Limits

Maximum allowed content length (Bytes): 300000000

Maximum URL length (Bytes): 4096

Maximum query string (Bytes): 2048

WebDAV adding MIME Type

If you have MIME types that you want all of your Web sites to recognize, you can add the new MIME types at the global level in IIS.
To add a global MIME type

1. In IIS Manager, expand the local computer, right-click the computer/site on which you want to add a MIME type, and click Properties.
2. Click MIME Types.
3. Click Add (or New).
4. In the Extension box, type the file name extension.
5. In the MIME type box, type a valid MIME type.

WebDAV create default MIME type

1. In IIS Manager, expand the local computer, right-click the computer/site on which you want to add a MIME type, and click Properties.
2. Click MIME Types.
3. Click Add (or New).
4. In the Extension box, type the file name extension.
5. In the MIME type box, type a valid MIME type.
    a. To create a MIME type for an undefined MIME type, type an asterisk in the Extension box, and type application/octet-stream in the MIME type box.
       Example: File name extension: '*' MIME type: application/octet-stream
    b. To create a MIME type for a file without an extension, type a period (.) in the Extension box, and type your MIME type in the MIME type box.
       Example: File name extension: '.' MIME type: application/octet-stream
6. Click OK.

Do not use wildcard MIME-types on production servers. Doing so can result in IIS serving unrecognized files and displaying sensitive information to users. Wildcard MIME-types are intended for testing purposes or in scenarios where Internet Server API (ISAPI) filters have been developed specifically to handle these wildcard scenarios, for example, a custom authentication ISAPI.

Set-up the Application Servers

Supported Windows versions

We support following Windows Application Server versions:

- Windows 2008 R2
- Windows 2012
- Windows 2012 R2
- Windows 2016
- Windows 2019

We recommend Windows 2012 R2 Application Server or newer, because it will use up to 5 times less network bandwidth than Windows 2008 R2, especially when using images inside the applications. This bandwidth saving is both from the Application Server to the Awingu VM as from the Awingu VM to the end-user's browser.

Notes:

- when using certificates on the application servers, the ones Windows generates are not compatible with Awingu.
- When using Windows 2008 R2 as application server, you need the optional update KB3080079: https://support.microsoft.com/en-us/kb/3080079

Enabling audio support

To enable audio in streamed applications, the Windows Audio Service needs to be enabled. To enable this service:

- Open Administrative Tools
- Open Services
- Open Windows Audio service
- Ensure that the service is running

Audio playback works on all supported browsers, except of Internet Explorer.

RDP vs RemoteApp

There are 2 methods to provide applications to Awingu:

- **Remote Application** is an extension to the Remote Desktop Protocol. Remote Application needs to be supported by your application server, and your applications need be exposed over Remote Application. It have has several advantages over the regular RDP applications:
  - The window selector (Windows button in the top of the app) is available.
  - The experience on tablets is smoother (especially when rotating the tablet and zooming in/out).
  - The app sharing experience is better.
  - It uses less resources on the application server.
- **RDP application** will make use of the regular Remote Desktop Protocol. **Full desktops** can only be provided via this protocol. If you provide an application (no full desktop) to Awingu, the user might notice a delayed closing of the session: after closing the application, a black screen can be shown for up to 3 minutes. This is because Windows keeps a print service running. To mitigate this behavior, please follow next solution: https://support.microsoft.com/en-us/help/2513330/

Windows 2008 R2 Application server

Please double check the Microsoft installation notes: http://technet.microsoft.com/en-us/library/dd883253%28v=ws.10%29.aspx

Install Remote Desktop Services

To install RD Session Host role service:

- Log on to Windows 2008R2 Server as Administrator.
- Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
- Under Roles Summary, click Add Roles.
- On the Before You Begin page of the Add Roles Wizard, click Next.
- On the Server Roles page, select the Remote Desktop Services check box, and click Next.
- On the Introduction to Remote Desktop Services page, click Next.
- On the Role Services page, select the Remote Desktop Session Host check box, and click Next.
- On the Uninstall and Reinstall Applications for Compatibility page, click Next.

- On the Specify Authentication Method for Remote Desktop Session Host page, click Don't Require Network Level Authentication, and click Next.
- On the Specify Licensing Mode page, select Configure later, and then click Next.
- On the Select User Groups Allowed Access To This Remote Desktop Session Host Server page, click Next.
- On the Configure Client Experience page, click Next.
- On the Confirm Installation Selections page, verify that the RD Session Host role service will be installed, and click Install.
- On the Installation Results page, you are prompted to restart the server to finish the installation process. Click Close, and then click Yes to restart the server.

> ✖ For Windows 2008 R2, you need following optional Windows Update to be applied in order to be compatible with Awingu: https://support.microsoft.com/en-us/kb/3080079

Configuration

Configure RemoteApp Setting

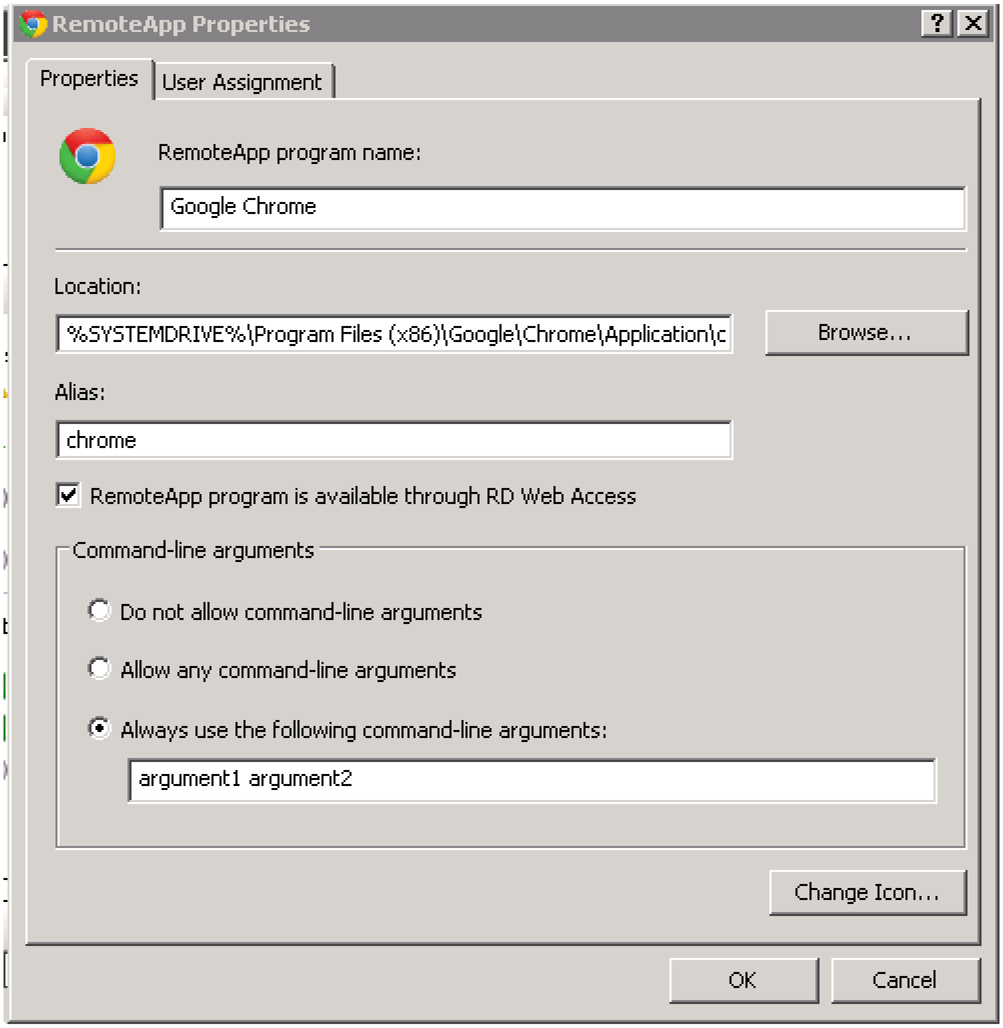
1. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
2. Under Roles, Remote Desktop Services, open RemoteApp Manager page, from the right menu select "Remote Session Host Server Setting".
3. Select "Do not allow users to start unlisted programs on initial connection", click Apply/OK
4. Under Roles, Remote Desktop Services, open RD Session Host Configuration page.
5. from edit setting, double click "Restrict each user to a single session", uncheck option, click OK.

Add/Remove RemoteApp programs

1. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
2. Under Roles, Remote Desktop Services, open RemoteApp Manager page, from right menu select "Add RemoteApp Programs".
3. On RemoteApp wizard, click Next, and select/browse for required programs to add, click Next.
4. Confirm required programs, click Finish

Additional Remarks

- Under "Roles -> Remote Desktop Services -> RemoteApp Manager" page you will find the list of all added RemoteApp programs.
- Make sure that all paths for added RemoteApp are absolute paths on the local system and not prefixed with the domain path.
  If applications doesn't have a correct path, double click the application in the list and edit the path.
  (E.g replace "\\appserver3.awingu.com\C$\Windows\System32\notepad.exe" with "C:\Windows\System32\notepad.exe")
- You can pass commadline arguments to your remoteApp by specifying them in your remoteApp properties tab as follows:



RemoteApp program name: Google Chrome

Location: %SYSTEMDRIVE%\Program Files (x86)\Google\Chrome\Application\c

Alias: chrome

☑ RemoteApp program is available through RD Web Access

Command-line arguments

○ Do not allow command-line arguments

○ Allow any command-line arguments

● Always use the following command-line arguments: argument1 argument2

Windows 2012 (R2), 2016 and 2019 Application server

Please refer to this guide: http://technet.microsoft.com/en-us/library/hh831447.aspx

Install Remote Desktop Services

1. Log on to Windows 2012/2016/2019 Server as Administrator.
2. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
3. From Dashboard, click "Add roles and features".
4. Select "Remote Desktop Services Installation", click Next.
5. From deployment type, select "Quick" deployment if you need to quickly deploy all roles to a single server. To have more control, use "Standard Deployment", click Next.
6. From deployment scenario, select "Session-based desktop deployment", click Next.
7. Finish and confirm Installation.
8. Restart the server.

Awingu will detect the the network level authentication for RDP connection automatically. This setting can be changed in the Server Manager, Remote Desktop Server Settings, deployment properties, security settings: Network Level Authentication can be enforced if desired.

If the Remote Desktop Connection Broker service is not running, we get following message when opening a streamed app to that application server: "The server denied the connection". Note that the app will start anyway. To avoid that message, please make sure the Remote Desktop Connection Broker service is running.

Configuration

Configure deployment service

1. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
2. Select "Remote Desktop Services".
3. From "DEPLOYMENT OVERVIEW", from the "TASKS" drop-down menu, click "Edit Deployment Properties".

4. From "RD Gateway", select "Automatically ...".
5. From RD Licensing, select "Per User", make sure that the Microsoft Remote Desktop Licensing Server is add to list, or add it.
6. click Apply/OK to finish.

Configure RemoteApp Collections

1. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
2. Select "Remote Desktop Services", select "Collections".
3. If you don't have any collections create new one, the default "QuickSessionCollection"
4. Make sure that network Level Authentication is not required.
    a. when on "QuickSessionCollection" on properties click tasks -> Edit properties
    b. Select Security,
    c. For the Security layer select negotiate.
    d. Encryption Level: Client Compatible
    e. Uncheck: Allow connections only from computers running Remote Desktop Service with Network Level Authentication

Configure RemoteApps

1. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
2. Select "Remote Desktop Services", select your collection "RemoteApps" from Collections.
3. From "REMOTEAPP PROGRAMS", from the "TASKS" drop-down menu, click "Publish RemoteApp Programs".
4. From "Publish RemoteApp Programs" form select the apps you want to be available.
5. For application interactivity (ex. edit files) you need to allow command line arguments:
   After publishing, go again to "REMOTEAPP PROGRAMS" section, check the properties of the published app and allow for command line arguments.

On Windows 2012/2016/2019 servers, the remoteapp alias cannot be changed through the GUI anymore. However, the remoteapp alias can still be changed via powershell.
In powershell you can use the following commands:

```
import-module RemoteDesktop
Set-RDRemoteApp -Alias "wordpad" -DisplayName "wordpad_Renamed"
```

Using Windows AD Administrative Center

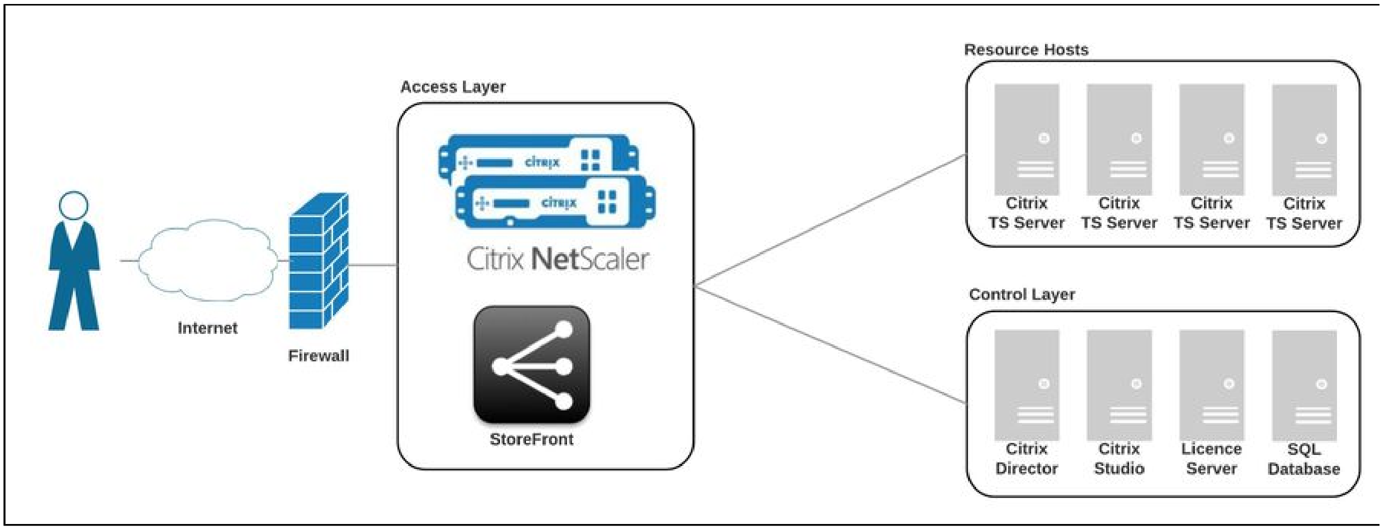
In Windows AD Administrative Center, the UPN is not required for a user. Awingu, however, requires this. Please provide a domain UPN as defined here: https://technet.microsoft.com/en-us/library/cc772007(v=ws.11).aspx

Using Awingu on existing Citrix infrastructure

Migrating away from an existing Citrix infrastructure to Awingu is one of our most asked questions. It's actually a real easy 4 step process. Simple & fast. We're describing it here below in full detail.

Note: There are a number of reasons why migrating from Citrix to Awingu is a good idea. We elaborate on this in more detail here.

Below is a picture of a typical Citrix XenApp Deployment:



Installing Awingu next to this setup can be achieved by deploying 1 (or more for load distribution or High Availability) Awingu appliance in the Access Layer following this procedure which can be executed in less than 1 hour.

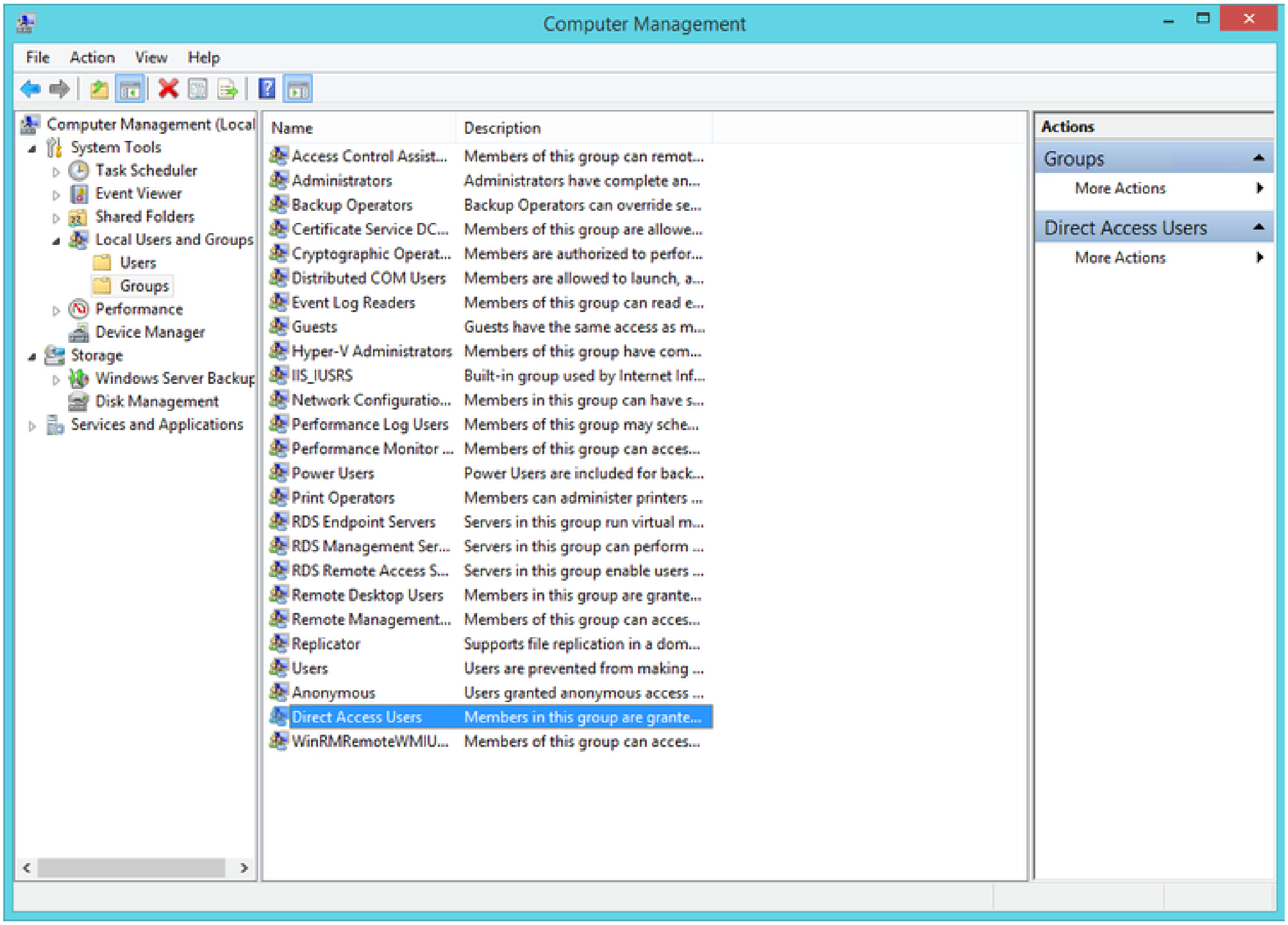
Note: as long Citrix is installed on the resource hosts, you need to have Citrix licenses for the RDP connections from Awingu to the resource hosts.

Preparation

Download, install and configure Awingu as described in Admin Guide. The Citrix TS Servers (Resource Hosts) are the application servers to configure in Application Server Management.

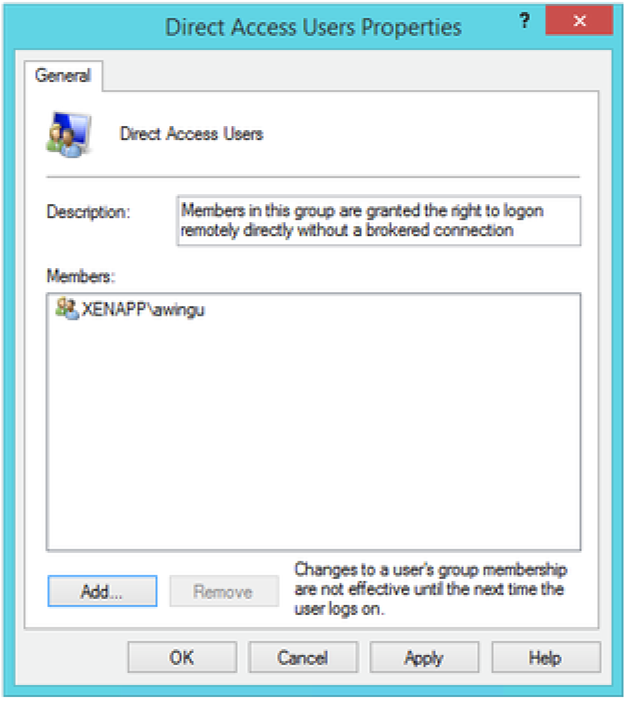
Allow non-administrators to RDP to the Citrix servers

When Citrix Virtual Delivery Agent is installed on a machine, non-administrators can no longer RDP to the machine. A new local group called Direct Access Users is created on each Virtual Delivery Agent. Add your non-administrator RDP users to this local group so they can RDP directly to the machine:



Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DC...	Members of this group are allowe...
Cryptographic Operat...	Members are authorized to perfor...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Print Operators	Members can administer printers ...
RDS Endpoint Servers	Servers in this group run virtual m...
RDS Management Ser...	Servers in this group can perform ...
RDS Remote Access S...	Servers in this group enable users ...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
Users	Users are prevented from making ...
Anonymous	Users granted anonymous access ...
Direct Access Users	Members in this group are grante...
WinRMRemoteWMIU...	Members of this group can acces...

Add here the security group for the users which should have access:



Direct Access Users

Description: Members in this group are granted the right to logon remotely directly without a brokered connection

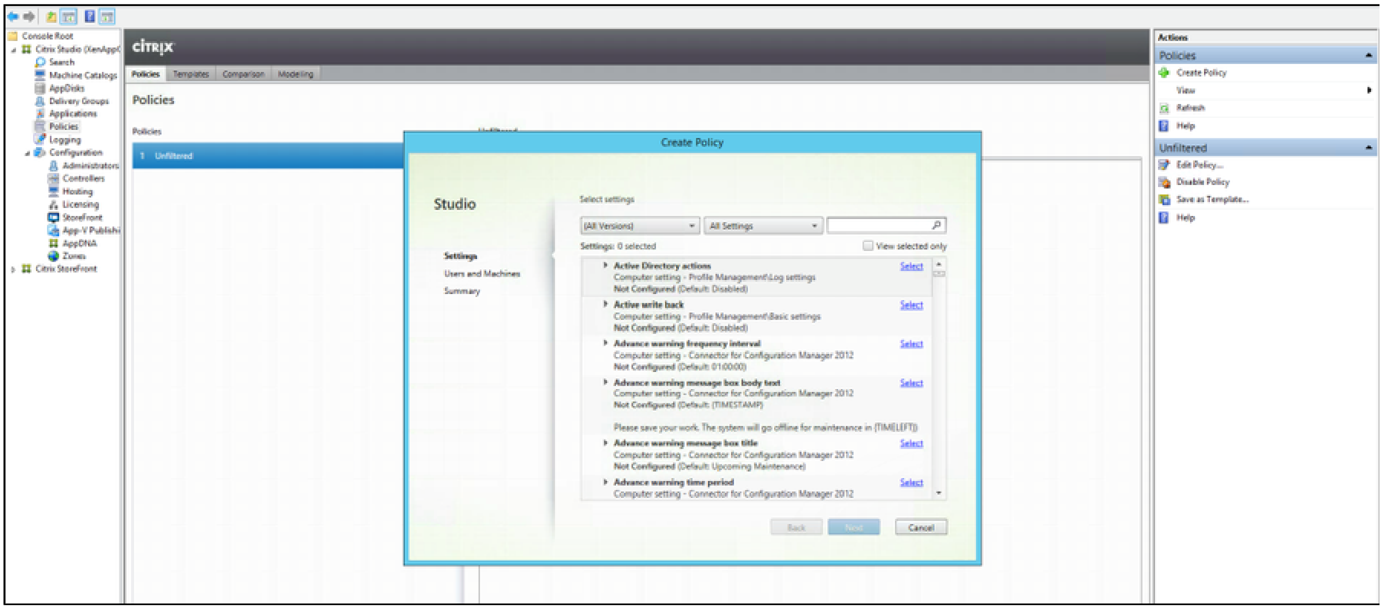
Members:

XENAPP\awingu

Changes to a user's group membership are not effective until the next time the user logs on.

Enable RDP policy in Citrix studio

To be able to initiate a remote session a policy needs to be added to Citrix. Open the Citrix director and browse to the policy section. On the right top choose Create Policy:



Select settings

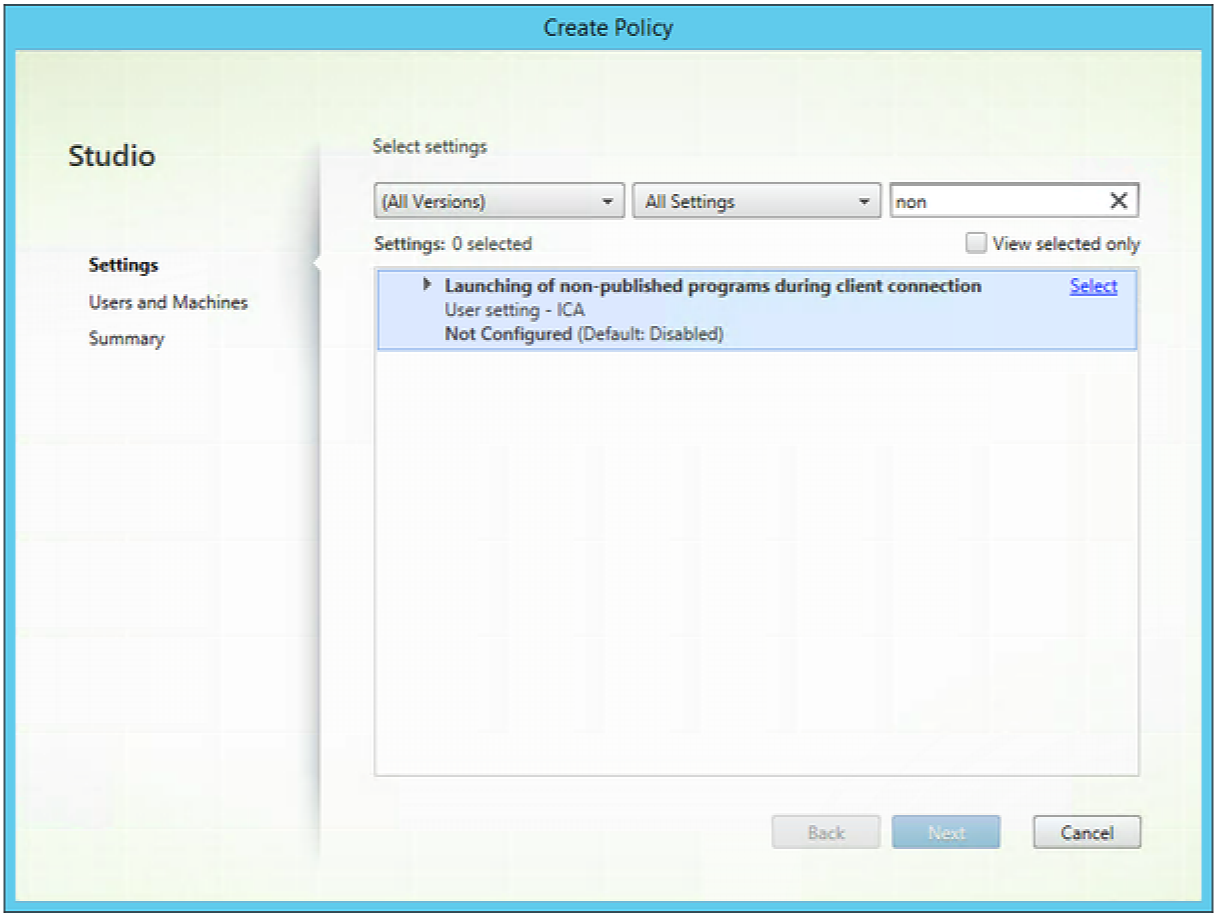
(All Versions) | All Settings

Settings: 0 selected ☐ View selected only

- **Active Directory actions** Select
  Computer setting - Profile Management\Log settings
  Not Configured (Default: Disabled)
- **Active write back** Select
  Computer setting - Profile Management\Basic settings
  Not Configured (Default: Disabled)
- **Advance warning frequency interval** Select
  Computer setting - Connector for Configuration Manager 2012
  Not Configured (Default: 01:00:00)
- **Advance warning message box body text** Select
  Computer setting - Connector for Configuration Manager 2012
  Not Configured (Default: {TIMESTAMP}

  Please save your work. The system will go offline for maintenance in {TIMELEFT})
- **Advance warning message box title** Select
  Computer setting - Connector for Configuration Manager 2012
  Not Configured (Default: Upcoming Maintenance)
- **Advance warning time period** Select
  Computer setting - Connector for Configuration Manager 2012

In the search field search for: "Launching of non-published programs during client connection" and select it:



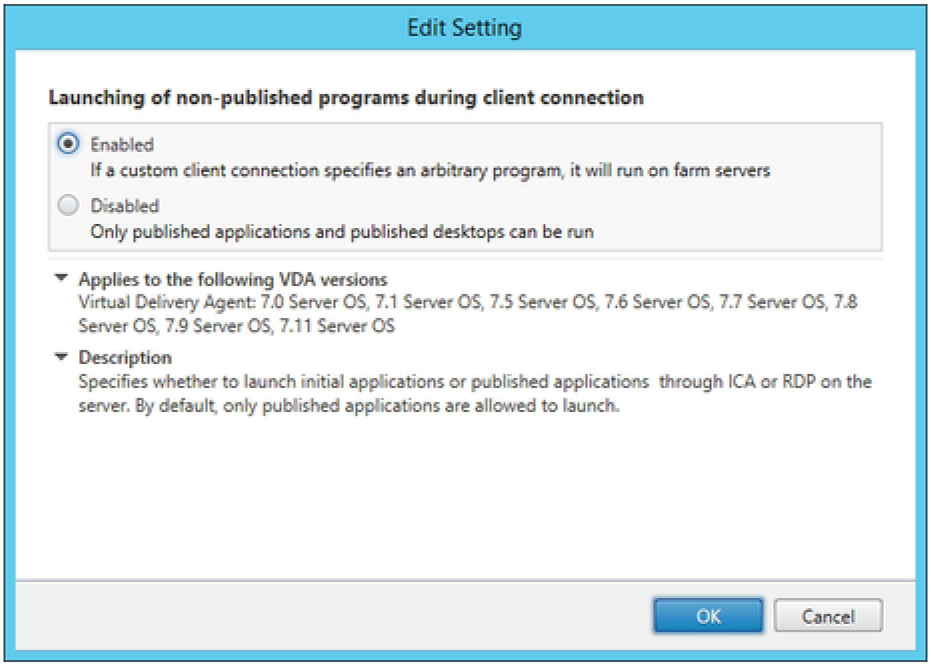
Select settings

(All Versions) | All Settings | non

Settings: 0 selected ☐ View selected only

- **Launching of non-published programs during client connection** Select
  User setting - ICA
  Not Configured (Default: Disabled)

Enable this policy for all objects in this site:



Edit Setting

Launching of non-published programs during client connection

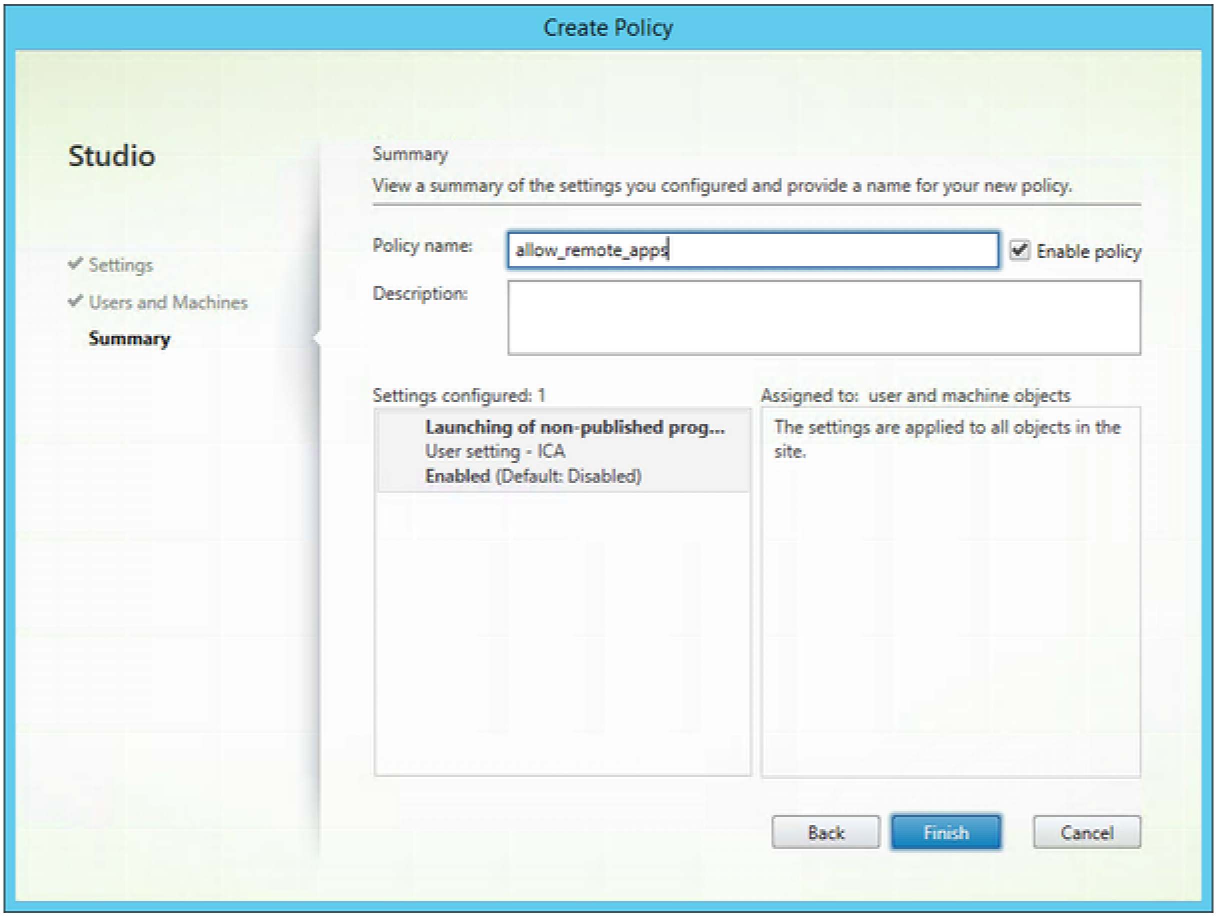
● Enabled
If a custom client connection specifies an arbitrary program, it will run on farm servers

○ Disabled
Only published applications and published desktops can be run

Applies to the following VDA versions
Virtual Delivery Agent: 7.0 Server OS, 7.1 Server OS, 7.5 Server OS, 7.6 Server OS, 7.7 Server OS, 7.8 Server OS, 7.9 Server OS, 7.11 Server OS

Description
Specifies whether to launch initial applications or published applications through ICA or RDP on the server. By default, only published applications are allowed to launch.

Give it a meaningful name and enable the policy:



Create Policy

Summary
View a summary of the settings you configured and provide a name for your new policy.

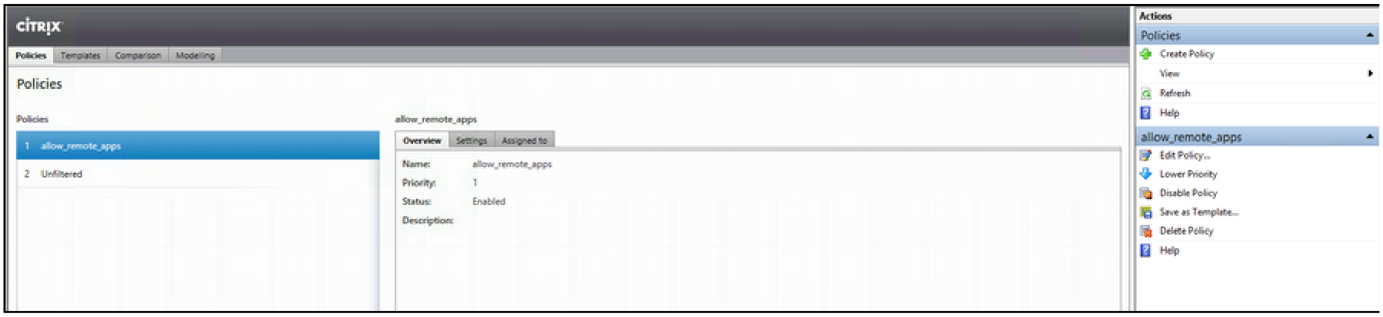
Policy name: allow_remote_apps ☑ Enable policy

Description:

Settings configured: 1
Launching of non-published prog...
User setting - ICA
Enabled (Default: Disabled)

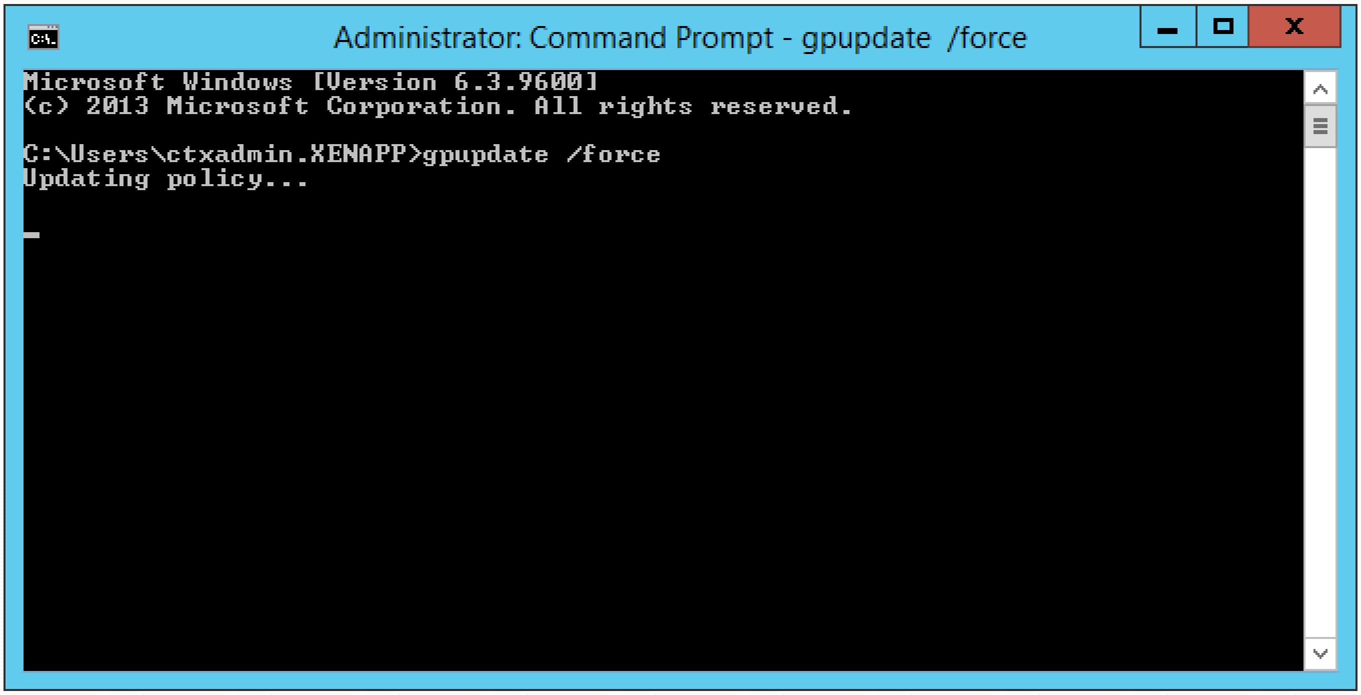
Assigned to: user and machine objects
The settings are applied to all objects in the site.

Set the policy priority higher:



Name: allow_remote_apps
Priority: 1
Status: Enabled
Description:

If you want to speed the policy up you can always update them manually:



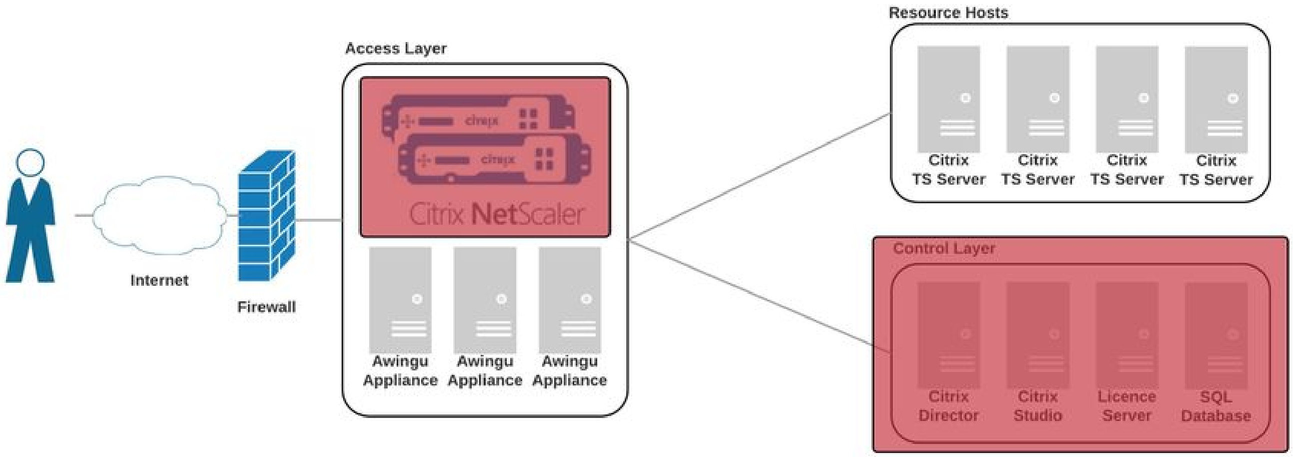
```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\ctxadmin.XENAPP>gpupdate /force
Updating policy...

_
```

Optional: uninstall Citrix software from app servers

The result would be like in following picture:



Please note that the Netscaler can be optionally used to loadbalance to the different Awingu appliances but any loadbalancer will do.

There is no need any more of the Citrix Control layer. The Awingu appliances have all knowledge needed to do the brokerage to the different RDS servers.

SSL offloader, reverse proxy or loadbalancer settings

Required Headers

WebSocket

WebSocket (WS) technology is based on upgrading a regular HTTP session to a long living WebSocket connection. To this end, the browser requests a protocol upgrade by sending a HTTP request with the headers for a protocol upgrade. Therefore, the proxy server needs to allows these headers to propagate, to ensure successful HTTP(S) to WS(S) upgrades

Header	Explanation
Connection	This value should be equal to Upgrade
Upgrade	Should be equal to websocket in case of an websocket upgrade

The connection header is a hop-by-hop header, it needs to be explicitly set by the SSL off-loader or proxy stages in between the browser and the Awingu environment. See the Nginx example below, to find the correct example settings.

This header only needs to be set to a limited set of URLs. These request are only request of the form /awingu/RDP, /awingu/JOIN and /awingu /API. For a multi node deployment, please replace awingu with the host names of the RDP Gateways. In general this can be triggered by the following regular expression: /.*/(RDP|API|JOIN).

SSL Offloader Headers

Header	Explanation
X-Forwarded-Proto	This is header is required to make share operational behind an SSL off-loader

Recommended Headers

These are settings that are known to work and they make sure the Awingu is aware of the proxy servers in front.

Header	Explanation
X-Real-IP	This should be the IP address of the requesting client
X-Forwarded-For	This should be the IP address of the requesting client
X-Forwarded-Host	This is the FQDN of the server name that was requested by the client
Host	This is the FQDN of the server name that was requested by the client

Proxy Timeout

Usually reverse proxies and SSL offloader have built-in times outs for their requests to back-end servers. In case of WebSockets however, a TCP connection is being kept open. Hence, one needs to make sure that the SSL off-loader or reverse proxies are not closing the connection after a few seconds or minutes of inactivity. This would results in streamed applications that are closings automatically for the end-user after this idle timeout value.

Please consult the documentation of your SSL offloader to change these settings in case of WebSocket. For Nginx based off-loading this setting is as follows:

```
### Proxy Read Timeout:
proxy_read_timeout 3500s;
```

Large File Uploads

Prior to version 4.1, Awingu accepted files up to maximum 100MB, and therefore the SSL and/or reverse proxies had to be configured to support of body size with this maximum size. For NGINX, this was achieved by setting the value of **client_max_body_size** to 101M. Since version 4.1 there is no upload size limit anymore, so the restriction can be omitted from the configuration.

Gzip compression

To reduce the size of transmitted data resulting in better performance, Awingu compresses it's HTTP(S) traffic using gzip. This is a standard supported by most browsers.
Awingu only compresses the data if the browser supports this, which is indicated by the presence of gzip in the Accept-Encoding header sent by the browser.

Please validate the Accept-Encoding header is not stripped by the reverse proxy, as this might result in performance loss.

Replacing Awingu Nodes

If an Awingu node with the **proxy** service enabled needs to be replaced, and you want to re-use the original IP address, then you need to remove that IP address from the reverse proxy/loadbalancer before you replace the node with a fresh Awingu appliance. If you don't, that new appliance will redirect port 80 to the 8080, where the installer is running.

After having added the new appliance to Awingu, you can re-add the IP address to the reverse proxy/loadbalancer.

Example NGINX Settings

> Due to the SSL 'logjam' vulnerability, you need to generate a new Diffie-Hellman group for TLS. For more information, please see https://weakdh.org/sysadmin.html.
> In order to generate a new Diffie-Hellman group, please use the following command:
>
> ```
> openssl dhparam -out dhparams.pem 2048
> ```
>
> After you have generated the new Diffie-Hellman group, you need to reference it in your Nginx configuration with the ssl_dhparam variable (see below).

The following config settings are working Nginx for SSL off-loading:

```
upstream frontends {
    server <IP-OF-AWINGU-VM>:80;
}

server {
    listen            80;
    server_name       sgo.yourcompany.com;
    ## redirect http to https ##
    rewrite        ^ https://$server_name$request_uri? permanent;
}

server {
    listen              443;
    ssl                 on;
    server_name         sgo.yourcompany.com;
    ssl_certificate     sslcerts/yourcompany.com.chained.crt;
    ssl_certificate_key sslcerts/yourcompany.com.key;
    # due to the SSL 'Poodle' vulnerability, SSLv3 should be disabled
    ssl_protocols       TLSv1.2 TLSv1.3;
    ssl_ecdh_curve      X25519:P-256:P-384:P-224:P-521;
    ssl_ciphers         EECDH+AESGCM:EDH+AESGCM;
    ssl_prefer_server_ciphers on;
    ssl_dhparam /etc/ssl/private/dhparams.pem;

    keepalive_timeout    60;
    ssl_session_cache    shared:SSL:10m;
    ssl_session_timeout  10m;

    # Gzip Settings
    gzip on;
    gzip_disable "msie6";
```

```
       gzip_types
           application/atom+xml
           application/javascript
           application/x-javascript
           application/json
           application/ld+json
           application/manifest+json
           application/rss+xml
           application/vnd.geo+json
           application/vnd.ms-fontobject
           application/x-font-ttf
           application/x-web-app-manifest+json
           application/xhtml+xml
           application/xml
           font/opentype
           image/bmp
           image/svg+xml
           image/x-icon
           text/cache-manifest
           text/css
           text/plain
           text/vcard
           text/vnd.rim.location.xloc
           text/vtt
           text/x-component
           text/x-cross-domain-policy;

       ### We want full access to SSL via backend ###
       location / {
                   proxy_pass  http://frontends;

                   ### force timeouts if one of backend is died ##
                   proxy_next_upstream error timeout invalid_header http_500 http_502 http_503 http_504;

                   ### Set headers ####
                   proxy_set_header        Accept-Encoding    "";
                   proxy_set_header        Host               $host;
                   proxy_set_header        X-Real-IP          $remote_addr;
                   proxy_set_header        X-Forwarded-Host   $host;
                   proxy_set_header        X-Forwarded-Server $host;
                   proxy_set_header        X-Forwarded-For    $proxy_add_x_forwarded_for;

                   ### Most PHP, Python, Rails, Java App can use this header ###
                   proxy_set_header        X-Forwarded-Protocol $scheme;
                   add_header              Front-End-Https   on;


                   ### By default we don't want to redirect it ####
                   proxy_redirect     off;

                   location ~ /.*/(RDP|API|JOIN|RAH) {
                       proxy_pass  http://frontends;

                       # WebSocket support (nginx 1.4)
                       proxy_http_version 1.1;
                       proxy_set_header Upgrade $http_upgrade;
                       proxy_set_header Connection "upgrade";
                       proxy_set_header        Accept-Encoding    "";
                       proxy_set_header        Host               $host;
                       proxy_set_header        X-Real-IP          $remote_addr;
                       proxy_set_header        X-Forwarded-Host   $host;
                       proxy_set_header        X-Forwarded-Server $host;
                       proxy_set_header        X-Forwarded-For    $proxy_add_x_forwarded_for;
                       ### Proxy Read Timeout: 12h
                       proxy_read_timeout 43200s;
                   }
      }
```

```
}
```

We recommend using minimum 512 worker connections per 50 concurrent users. This can be configured in /etc/nginx/nginx.conf. For the number of open files, take some additional margin. Example for **200 users**:

```
worker_rlimit_nofile 3000;

events {
        worker_connections 2048;
}
```

Multi Factor Authentication

Using Awingu built-in OTP

Introduction

Awingu has a built-in Multi-Factor Authentication (MFA) option: counter based OTP (one time password):

- The first time a users logs in, they have to configure an application on their smartphone.
- Each next time they log in, they have to provide a token generated in that application.

Note that the OTP token will also be asked when required to login when using Awingu as Identity Provider or as Reverse Proxy.

Configuration

OTP can be enabled for each domain, cf. User Connector Configuration: in the Multi-Factor Authentication section, enable the option *Counter based OTP (builtin)*. Optionally, the admin can choose to allow users to remember their device for 30 days or to whitelist some networks. In those cases, no OTP token will be asked at login.

The button *Manage User Token Count* allows the admin to reset the token count for specific users. When the token is reset, the user will need to set-up their device again.

User Set-Up

The first time a user wants to login, they need to do following steps:

1. Download an application supporting counter based one-time password generation (typically on their smartphone).
   a. iOS and Android: Google Authenticator (iOS/Android)
   b. Windows Phone: Auth7
2. After providing credentials on the Awingu login page, the user will be forwarded to a page showing a QR code and a secret.
3. The user scans the QR code with their phone (or enters the secret manually).
4. The first token is generated in the app. The user enters that token to proceed.

Every next time the user logs in, they only need to provide their token.

Integrating Awingu with DUO

Introduction

Awingu integrates with Duo for multi-factor authentication.

This guide will walk you through the different steps required to configure both Awingu and Duo to enable the integration.

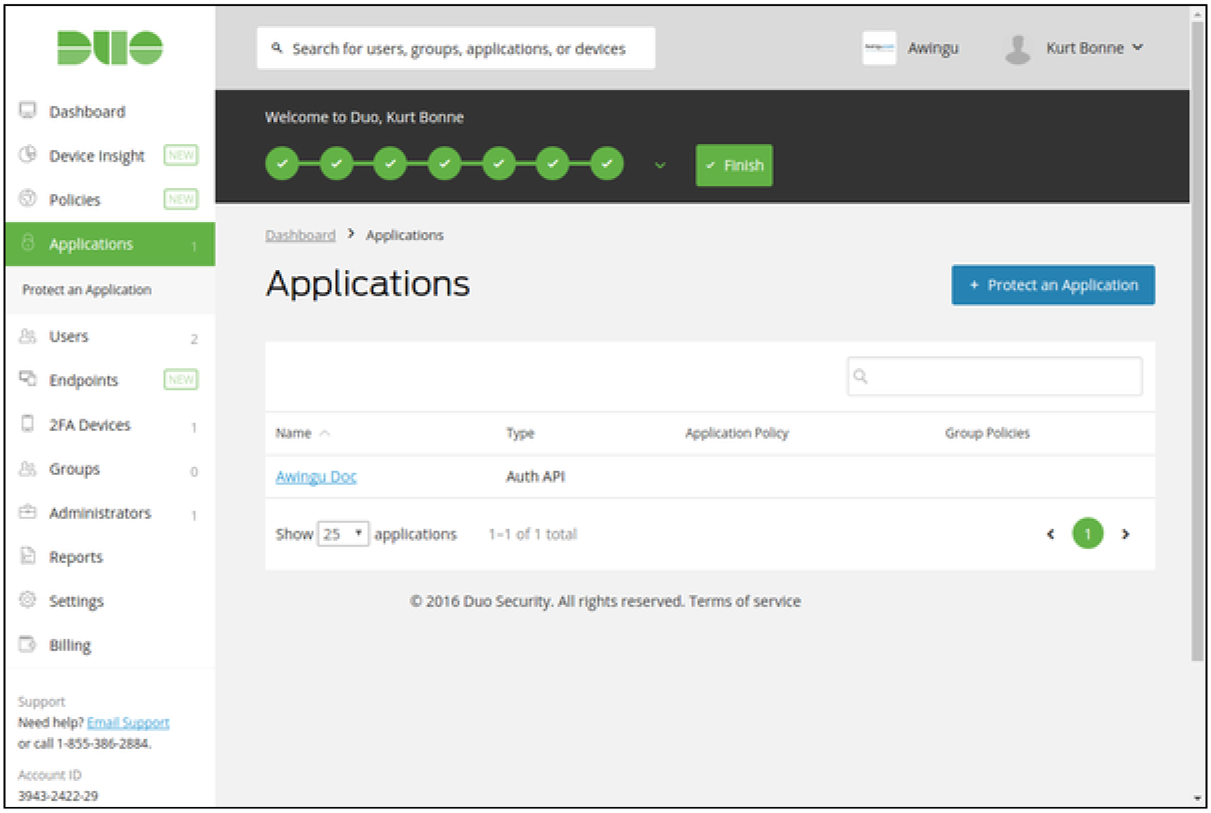
Prerequisites

This guide assumes you have administrative access to a working Awingu environment and an active Duo account. The Duo personal plan is sufficient to evaluate Duo integration with Awingu.

As Duo is a SaaS service, the Awingu environment requires access to the Duo SaaS service. This is `TCP 443` to the API hostname of your configured application (<your_api>.duosecurity.com).

Configuring your Awingu application in Duo

Sign-in to your Duo account and select `Applications` in the menu.

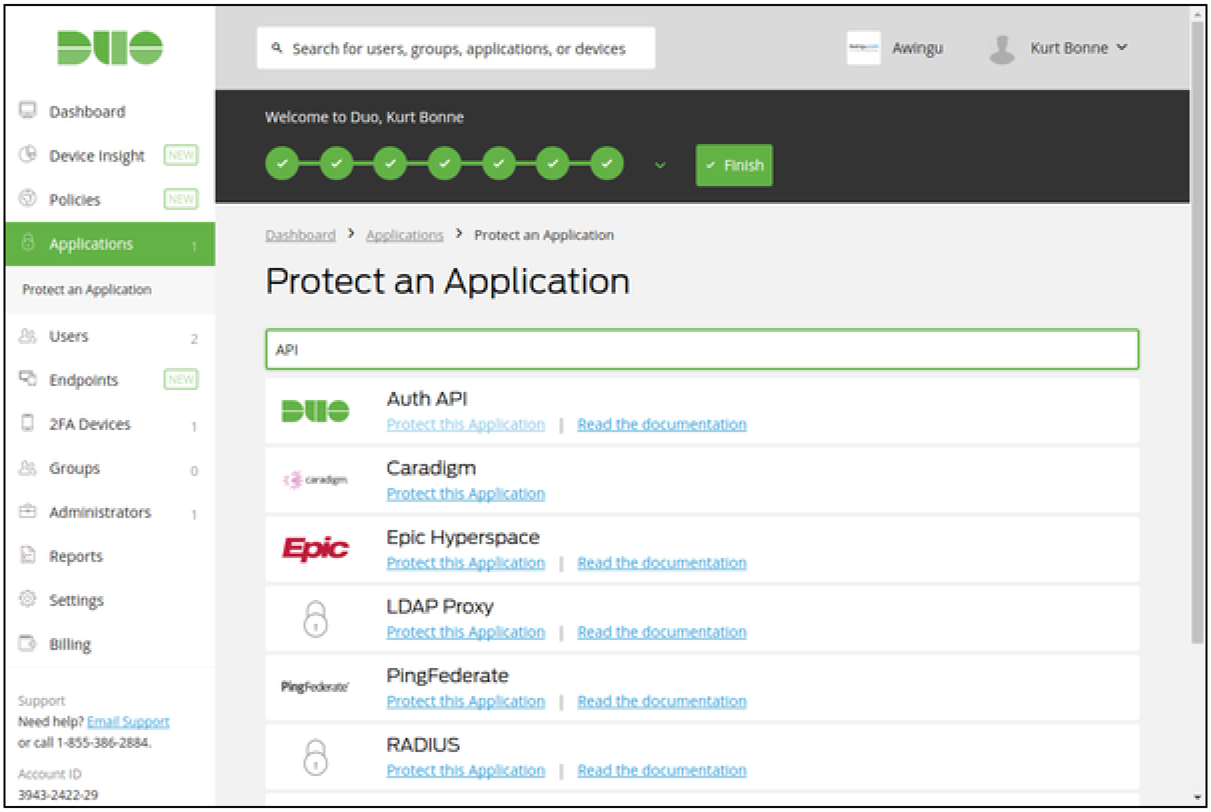


Name	Type	Application Policy	Group Policies
Awingu Doc	Auth API		

Show 25 applications 1-1 of 1 total

© 2016 Duo Security. All rights reserved. Terms of service

To add you Awingu application, click *Protect an Application* and select *Auth API* as type.



Support
Need help? Email Support
or call 1-855-386-2884.

Account ID
3943-2422-29

Welcome to Duo, Kurt Bonne

Dashboard > Applications > Protect an Application

Protect an Application

API

Auth API
Protect this Application | Read the documentation

Caradigm
Protect this Application

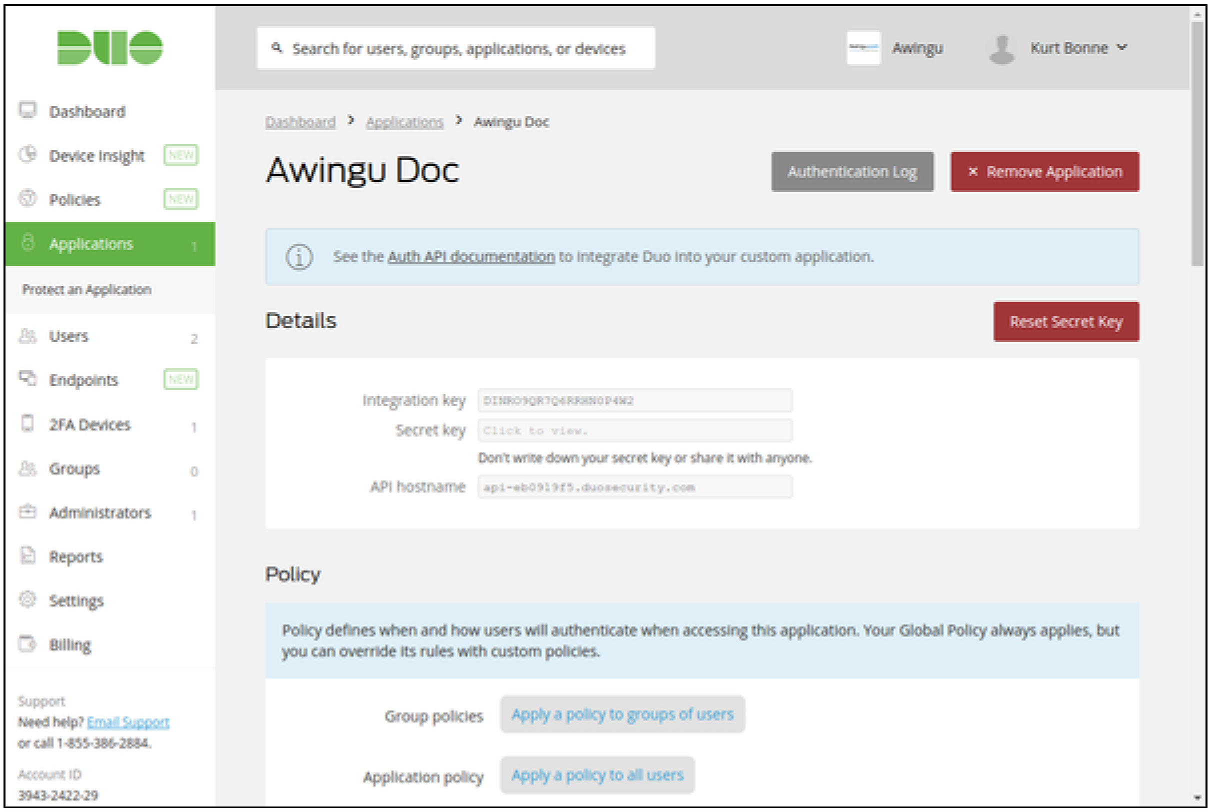
Epic Hyperspace
Protect this Application | Read the documentation

LDAP Proxy
Protect this Application | Read the documentation

PingFederate
Protect this Application | Read the documentation

RADIUS
Protect this Application | Read the documentation

This will result in a pre-configured application in Duo. The *Details* section of the application provides you with all details required to configure Awingu later on.



Support
Need help? Email Support
or call 1-855-386-2884.

Account ID
3943-2422-29

Dashboard > Applications > Awingu Doc

Awingu Doc

See the Auth API documentation to integrate Duo into your custom application.

Details

Integration key DINRO9QR7Q6RRHN0P4W2
Secret key Click to view.
Don't write down your secret key or share it with anyone.
API hostname api-eb0919f5.duosecurity.com

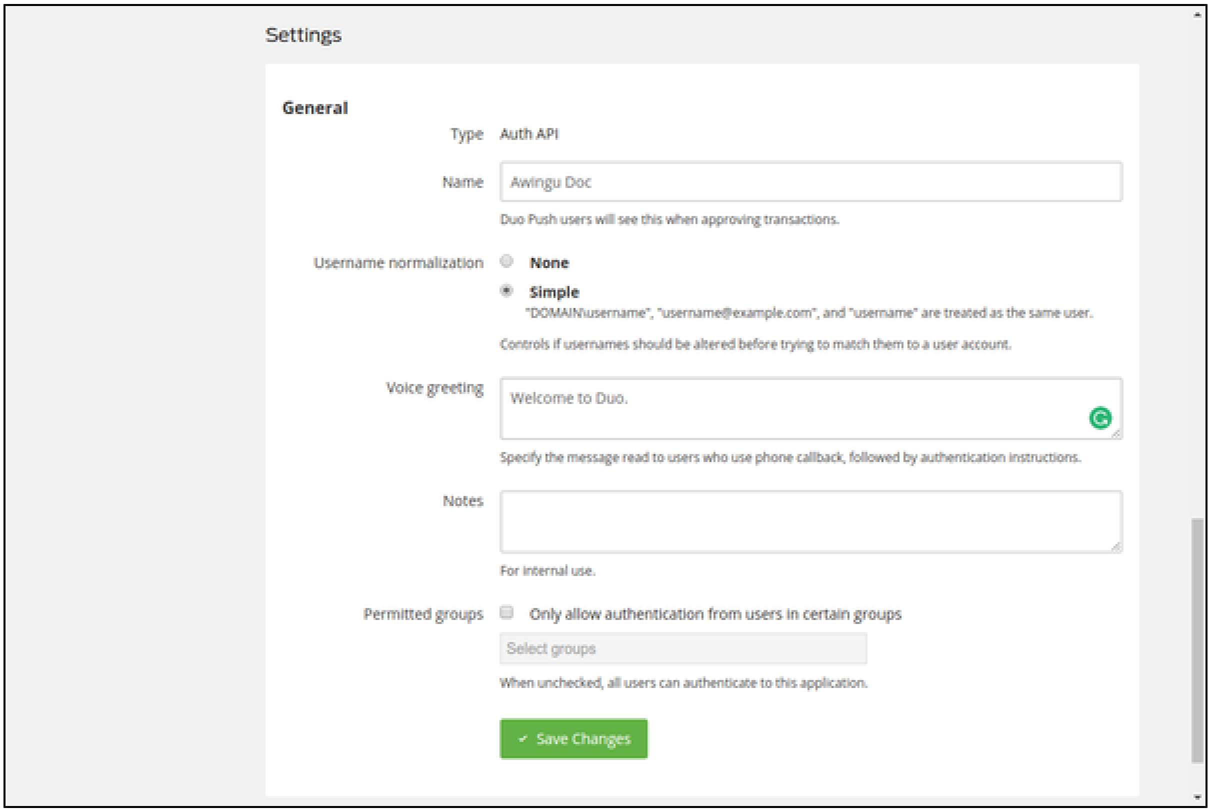
Policy

Policy defines when and how users will authenticate when accessing this application. Your Global Policy always applies, but you can override its rules with custom policies.

Group policies Apply a policy to groups of users

Application policy Apply a policy to all users

Before moving over to configure Awingu, we need to change some default values of the Duo settings in the *General* section.



Settings

General

Type: Auth API

Name: Awingu Doc

Duo Push users will see this when approving transactions.

Username normalization: ○ **None** ● **Simple**

"DOMAIN\username", "username@example.com", and "username" are treated as the same user.

Controls if usernames should be altered before trying to match them to a user account.

Voice greeting: Welcome to Duo.

Specify the message read to users who use phone callback, followed by authentication instructions.

Notes:

For internal use.

Permitted groups: □ Only allow authentication from users in certain groups

Select groups

When unchecked, all users can authenticate to this application.

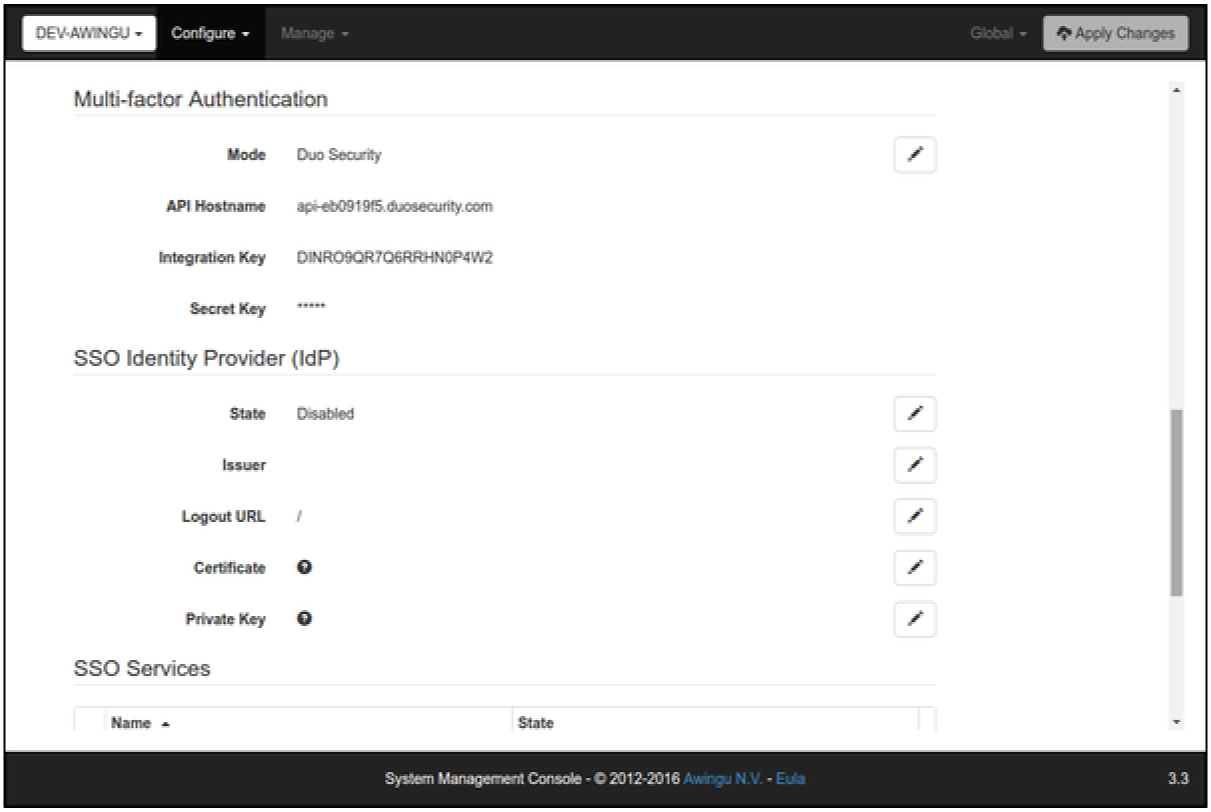
Please make sure the *simple* username normalization is enabled, or all authentication requests will fail. In this section you can also provide a more meaningful name for your Duo Awingu application.

Save your changes and your Duo application is Awingu ready.

Configuring Duo in Awingu

To configure MFA in Awingu, navigate to *Configure* > *User Connector* for your domain. Please be aware that the MFA configuration is domain specific.

Scroll down to the *Multi-factor Authentication* section and select the *Duo Security* mode.



Multi-factor Authentication

Mode	Duo Security
API Hostname	api-eb0919f5.duosecurity.com
Integration Key	DINRO9QR7Q6RRHN0P4W2
Secret Key	*****

SSO Identity Provider (IdP)

State	Disabled
Issuer	
Logout URL	/
Certificate	
Private Key	

SSO Services

Name	State

Enter the beforementioned corresponding values from the Duo portal and press apply.

Now Awingu is configured to use *Duo* as MFA provider for all users of the selected domain!

Users

To enable *Duo* MFA for your users, the users should be enrolled with *Duo*. These can be enrolled manually, imported or synced with Active Direct.

Please have a look at Duo's *Enrolling Users* documentation (https://duo.com/docs/enrolling_users) to see what option fits best your use case.

Known Limitations

- Awingu **does not support users with status bypass**
  Duo provides a feature that allows you to configure users to skip MFA. This can be done be setting the user's status to `bypass`. Awingu does not honour this status and thus will prevent the user to sign in.

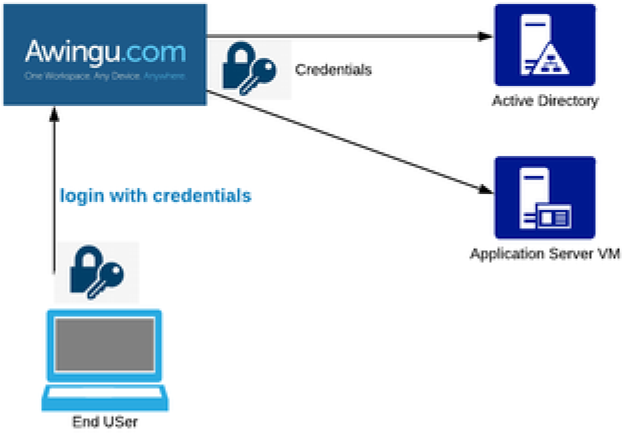
Awingu Single Sign On (SSO)

Next to the standard username/password login, Awingu is also able to do a full Single Sign-on (SSO) via an external Identity Provider.

How does it work?

Standard Login

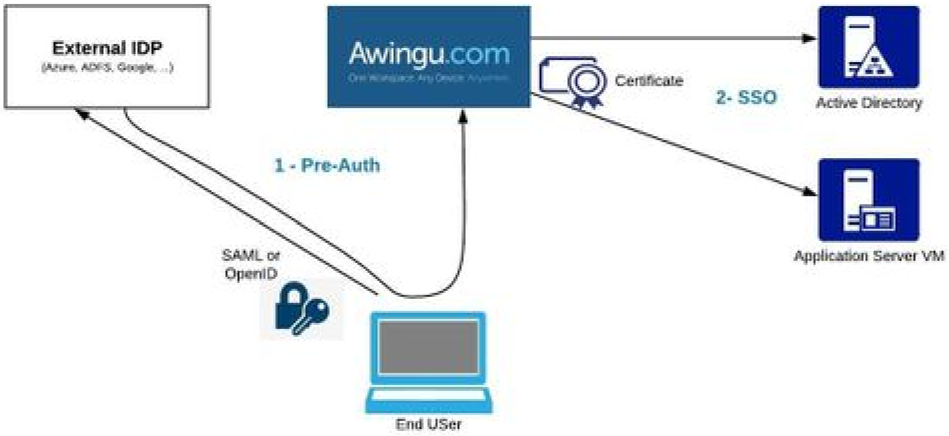
In the *standard setup* Awingu validates directly with the Active Directory (AD) if the username/password provided in the Awingu login page is correct. To do this it makes a connection over LDAP(s) and if the credentials are fine it will fetch over LDAP(s) the security groups of the user and build up the Awingu user profile and landing page. When starting a virtual desktop (VDI) or a remote application (remote app) the credentials are transparently injected into the RDP stream and the VDI or remote app is started.



SSO Login

When switching to *SSO* the login becomes a 2 step process.

Firstly Awingu no longer does the authentication of the user itself, but this is handled by an external Identity Provider (IDP). As the external IDP doesn't expose the passwords and the Microsoft Remote Desktop Protocol (RDP) doesn't support ticket/token based logins, in a second step, the credential based logins towards back-end systems (remote app, VDI, storage, ...) is replaced by a certificate based login mechanism.



Configuration

To setup Single Sign-On several steps need to be completed.

1. Enable pre-Authentication
    a. Add Awingu as a trusted application into your IDP
        i. Azure AD

ii. Microsoft ADFS
iii. Google ID

b. Configure Awingu for SAML or OpenID connect authentication
c. Test & Troubleshoot pre-authentication

2. Enable Single Sign-On
   a. Generate Certificate & Setup the intermediate Sub-CA
   b. Validate if Windows backend is correctly configured for Awingu SSO
   c. Configure Awingu for SSO

Pre-authentication against an external IDP is possible for SAML (v2) and OpenID Connect based IDP's.

In general Awingu should be compatible with any IDP that supports these standards. In this manual we describe how to do the setup for following tested IDP's:

- Azure AD (via SAML)
- ADFS (via SAML)
- Google (via OpenID Connect)

End User Flow:

- When a user accesses the Awingu landing page, Awingu will check if the user has a valid authentication token with the configured IDP.
- If this is not the case yet, Awingu will redirect the browser to the IDP. The user will need to authenticate first against the IDP. If successful the IDP will redirect the User to the Awingu landing page.
- Awingu will ask the user for their Windows password.
- User will be logged in to the Awingu Workspace
- From the Workspace they can start Apps, Desktops and get access to the Drives.

From a technical point of view Awingu needs a valid SAML or OpenID Connect ticket before it allows the user to login to the Awingu portal. As the Microsoft RDP protocol doesn't support SAML or any other ticket based login mechanisms and as the IDP doesn't expose or include the entered password inside the ticket, the user needs to enter his Windows password (again) before he can login to the Awingu portal. The login into the portal and the apps happens via the standard credential based authentication mechanism.

To get the extra "windows password" removed you need to upgrade from pre-auth to SSO.

Use Cases:

By enabling this pre-authentication you can enable some extra use cases:

Conditional Access

Awingu allows access from any device. For some organizations this is not desired and they want to limit access to only managed devices. Via a firewall or reverse proxy in front of Awingu you can already do some first filtering (for example only allow connections from a specific range of IP addresses) but thanks to the pre-authentication you can use the conditional access features of your IDP to, for example, limit access to Awingu so login can only be done on managed devices.

See https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/require-managed-devices on how to do this when using Awingu in combination with Azure AD.

Azure MFA or other MFA solutions not compatible with radius

Awingu has a built-in connector for Azure MFA but it relies on the Azure MFA Server. This is a local windows machine you need to install that has an API that can be used to validate user logins against Azure MFA. Unfortunately Microsoft has deprecated this Azure MFA Server solution and as there is no open API available to integrate directly with Azure MFA the only remaining solution is to do Azure MFA validation via SAML.

The Awingu MFA plugin for Azure will probably be removed in a future version of Awingu.

Add Awingu as a trusted application into your IDP

Awingu can work with any external IDP that supports SAML or OpenID Connect. Please check the documentation of your IDP on how to add a trusted application.

Azure AD, Azure AD with OPSWAT, Microsoft ADFS & Google have been tested in combination with Awingu.

Please check following documentation on how to configure them:

- Setting up Azure AD as an external IDP for Awingu
- Setting up Azure AD with OPSWAT as external IDPs for Awingu
- Setting up Microsoft ADFS as an external IDP for Awingu
- Setting up Google as an external IDP for Awingu

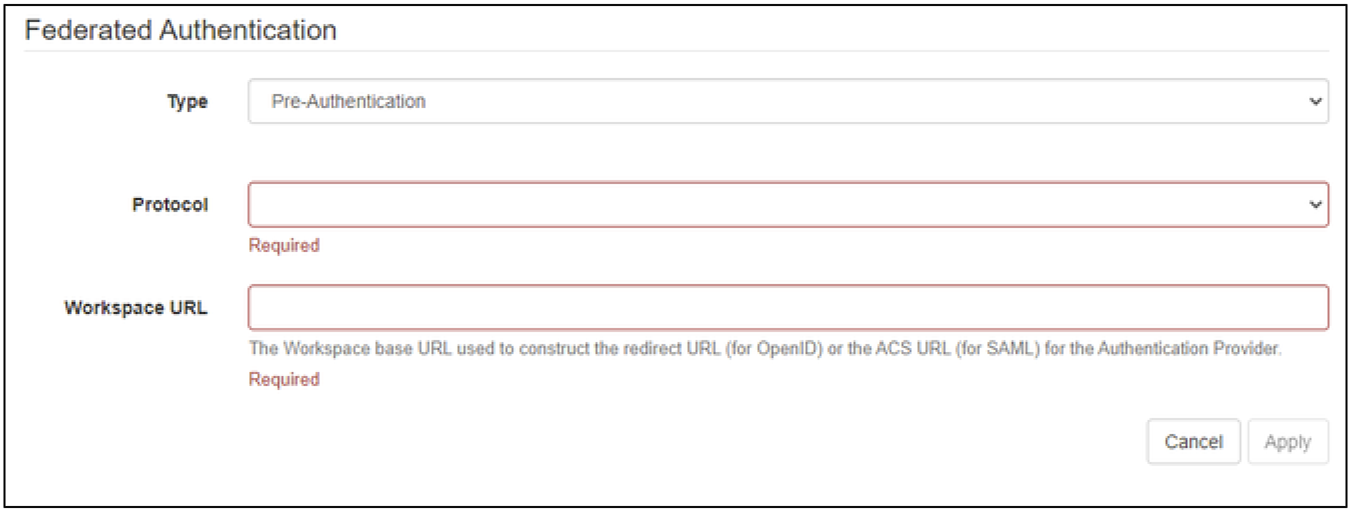
Configure Pre-Authentication

Before you start configuring the pre-authentication make sure there is a host header set on the tenant. Goto "global" "Domains" Select your domain. Make sure in the list of host headers for this domain the public DNS name of the Awingu environment is set. So for example if your public url for your Awingu environment is https://awingu.company.com make sure that in the list of host headers "awingu.company.com" is set.

To start the configuration itself of the pre-authentication, login to Awingu as an admin and open the system settings: Go to "Configure"   "User Connector" "Federated Authentication"

Set:

- Type to "Pre-Authentication"
- Select the correct protocol: SAML, SAML with Intermediate IdP or OpenID
- Provide the URL pointing to your Awingu environment. This URL will be used to construct the return URL you will need in the configuration of the IDP. (for example https://awingu.company.com/)



Federated Authentication

Type: Pre-Authentication

Protocol:

Required

Workspace URL:

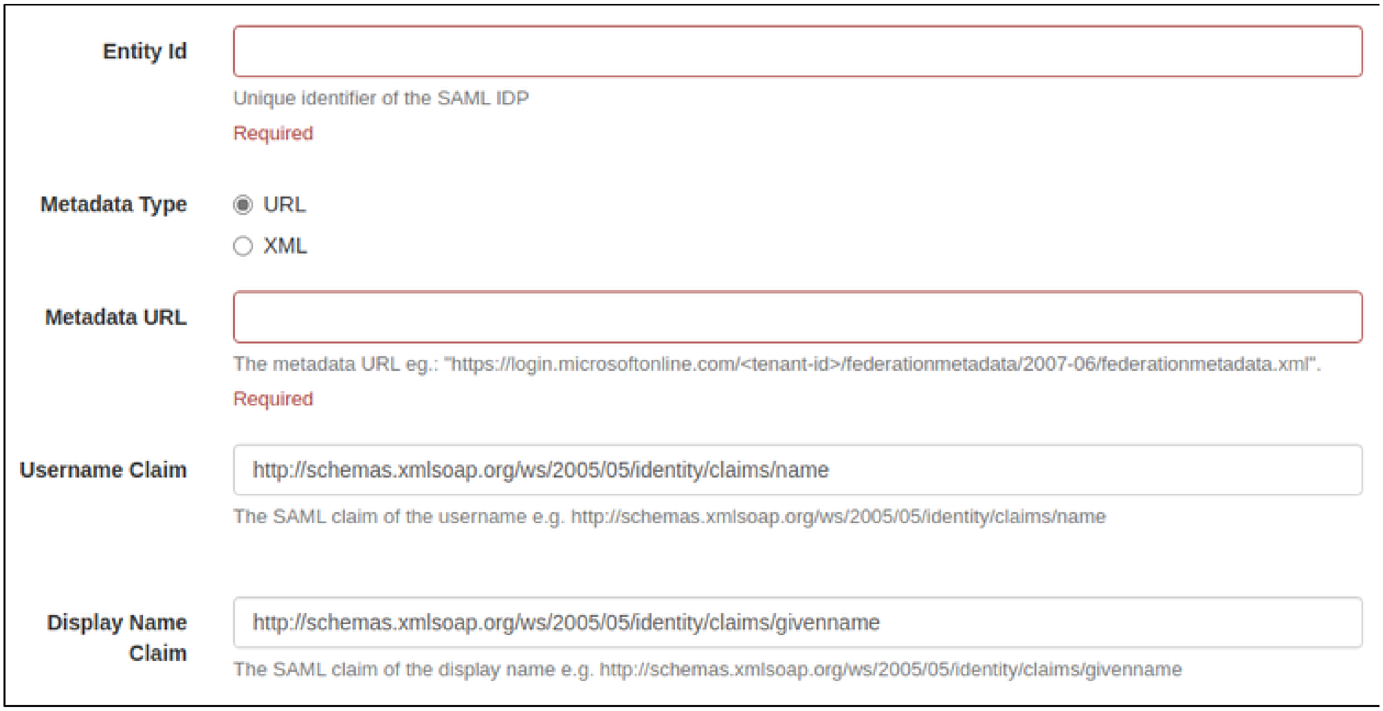
The Workspace base URL used to construct the redirect URL (for OpenID) or the ACS URL (for SAML) for the Authentication Provider.

Required

Configure Pre-Authentication with SAML

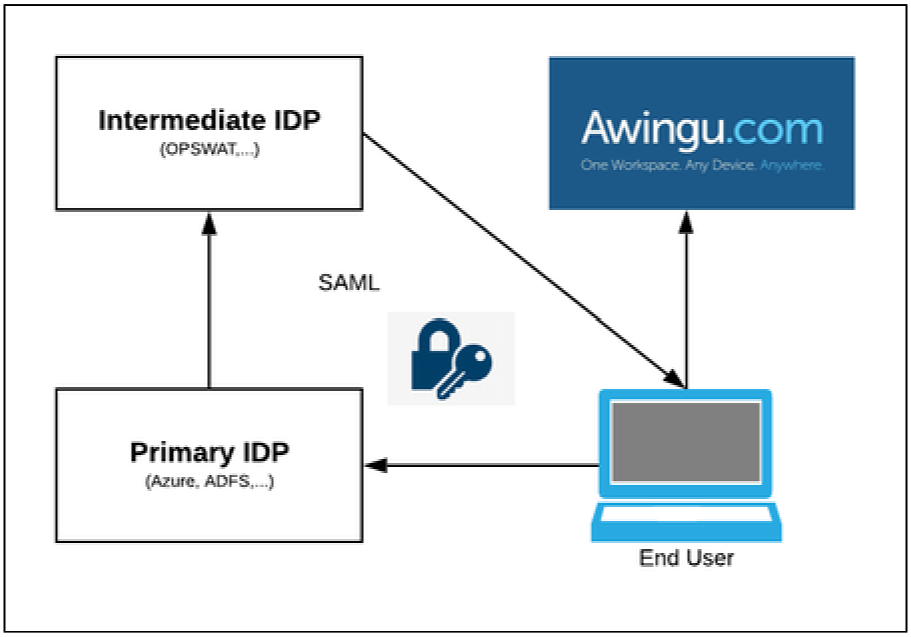
To use SAML for an external IDP the following fields need to be provided:

- **Entity Id:** The unique identifier on your IDP for the Awingu application.
  - For Azure AD this is "**spn:**<application-id>" (example spn:1234-5678-90xxxx). The Application ID is a property of the Azure Application (see Setting Up Azure AD as an external IDP for Awingu)
  - For ADFS this is the relying party identifier configured when setting up your relying party trust in ADFS (see Setting Up ADFS as an external IDP for Awingu)
- **Metadata Type:** How is the SAML Federation Metadata provided? Depending on the capabilities of the used Identity Provider.
  - URL: The appliance should download the metadata at every login attempt using a provided URL.
  - XML: The metadata is uploaded as a static .XML file.
- **Metadata URL:** The URL of the federation metadata document. When using https please make sure the URL is accessible via a public trusted certificate. If your certificate is not publicly trusted then you can host the metadata.xml file on another web server as a workaround.
- **Metadata XML:** The .xml file providing the federation metadata to upload to the appliance.
- **Single Logout:** Enable to also log the user out of the IdP if he logs out of this workspace. Requires configuration on the Identity Provider. See the documentation: Setting up Azure AD as an external IDP for Awingu
- **Username Claim URL:** The SAML response received by Awingu contains different properties (e.g. email, UPN, sAMAccountName, display name,..). Using the Username Claim URL you can specify which property will be used when logging into Awingu. When Single Sign-On (SSO) is enabled, the Username Claim URL needs to be set to the UPN.
  - When using Azure AD the default value is used (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name).
  - When using ADFS it is best to directly use the UPN (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn).
- **Display Claim URL** will be used on the login page of Awingu when the user successfully logged into the identity provider (e.g. "Welcome David"). The default value will be the claim URL to the given name (http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname) pr operty. Possible other claims URI's can be found here: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/technical-reference/the-role-of-claims



Entity Id	 Unique identifier of the SAML IDP Required
Metadata Type	● URL ○ XML
Metadata URL	 The metadata URL eg.: "https://login.microsoftonline.com/<tenant-id>/federationmetadata/2007-06/federationmetadata.xml". Required
Username Claim	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name The SAML claim of the username e.g. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name
Display Name Claim	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname The SAML claim of the display name e.g. http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname

Configure Pre-Authentication with SAML and Intermediate IdP



SAML Login flow when using an intermediate IdP:

- When a user accesses the Awingu landing page, the user will be redirected to the Primary IDP.
- After the user logs in to the Primary IDP, he will be redirected to the Intermediate IDP (Intermediate ACS URL).
- The Intermediate IDP can perform additional checks (device compliance, monitoring, credentials,..).
- When the Intermediate IDP allows the user through, it will redirect him to Awingu (ACS URL).
- Awingu then determines if the user is successfully pre-authenticated by validating the SAML response from the Intermediate IDP (using the Intermediate Signing Certificate).

To use SAML with an intermediate IDP the following extra fields need to be provided:

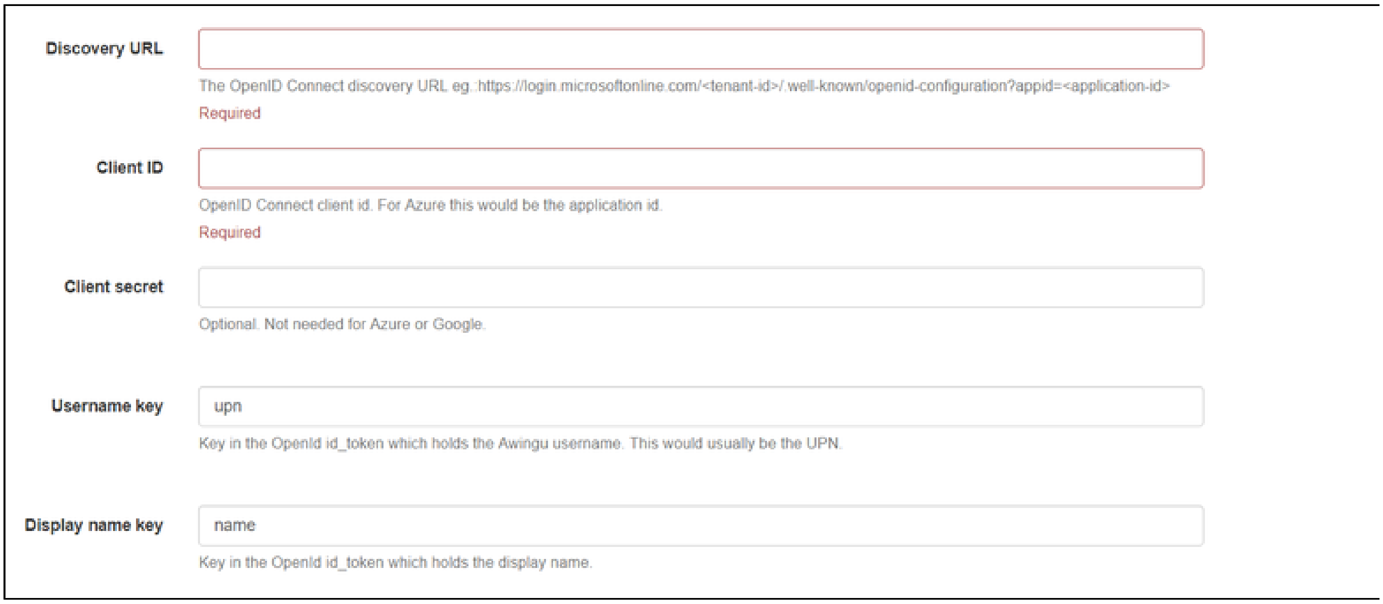
- **Intermediate ACS URL:** The Primary IDP redirects to this URL in case of successful authentication.
- **Intermediate Signing Certificate:** Awingu uses this certificate to check the SAML response from the Intermediate IDP.

See Setting up Azure AD with OPSWAT as external IDPs for Awingu for an example configuration where Azure AD is used as the Primary IDP and OPSWAT as the Intermediate IDP.

Configure Pre-Authentication with OpenID

To use OpenID for an external IDP the following fields need to be provided:

- **Discover URL:** The OpenID Connect discovery URL.
  - For google this is: https://accounts.google.com/.well-known/openid-configuration (See https://developers.google.com/identity/protocols/OpenIDConnect for more details)
- **Client ID:** OpenID connect client ID
- **Client secret:** *Optional*. For Google & Azure this is not needed and can be left blank
- **IdP Logout URL:** *Optional*. When an URL is provided to logout the user from the IdP, Awingu will redirect to it after the user logs out of Awingu. E.g. when using Google as IdP this could be https://www.google.com/accounts/Logout.
- **Username key:** Key in the Open id_token which holds the Awingu username.
  - For Google use email
  - For Azure use upn
- **Display name key:** Key in the Open id_token which holds the display name
  - For Google use email
  - For Azure use name



Discovery URL

The OpenID Connect discovery URL eg.:https://login.microsoftonline.com/<tenant-id>/.well-known/openid-configuration?appid=<application-id>

Required

Client ID

OpenID Connect client id. For Azure this would be the application id.

Required

Client secret

Optional. Not needed for Azure or Google.

Username key: upn

Key in the OpenId id_token which holds the Awingu username. This would usually be the UPN.

Display name key: name

Key in the OpenId id_token which holds the display name.

Testing & troubleshooting pre-authentication

When testing pre-authentication for the first time please make sure you use an inprivate or incognito browser window. In some cases there might still be active cookies in your main browser window that prevent the correct login.

If pre-authentication works via incognito windows but not via your normal browser window then delete your browser cookies from today.

If the configuration is done correctly both on the IDP as well as in the Awingu configuration you should experience the correct end user flow as described above.

In the event of an issue, this chapter will help you in troubleshooting. We have documented the most common issues.

How to access the system settings when pre-auth has a faulty configuration?

Once pre-authentication is enabled, all windows based accounts will need to first authenticate against the IDP before they can login to Awingu. In the event of an issue with the IDP configuration or Awingu configuration, the following procedures can be used to access the Awingu system settings. All these procedures **assume that you execute them in an inprivate/incognito browser window** and will only work for **the built-in Awingu admin user**.

1. Access the Awingu appliance on a different URL than the one that is linked to your IDP:
   a. In case of a multi-tenant setup login to another tenant where no pre-auth is configured. In this case the tenant must also be administrative to allow modification to the impacted tenant. This procedure will also work with all admin users on the other tenant.
   b. In case of a single tenant or multi-tenant without other administrative domains add a new/other DNS record for the system or try to connect with the IP rather than the DNS name. In this case there might be certificate issues or the extra DNS names may not exist on a reverse proxy in front of Awingu.

2. Access the Awingu appliance via the "noPreAuth" flag: Assuming your Awingu URL is https://awingu.company.com - by going to https://awingu.company.com/login?noPreAuth (**case sensitive!!**) you will get the login prompt with username / password. As previously mentioned this login will only work with the built-in Awingu admin user.

Awingu doesn't do a redirect to my IDP

When a user goes to Awingu the redirect to the IDP is not working. Instead of being redirected to the IDP the user gets a login/password prompt and when typing in their username / password an error is shown stating that pre-authentication is required.

This issue mostly happens when either

1. There is no (or faulty) host header set in the domain settings of Awingu for this tenant. (global domains).
2. Awingu can't access/read the metadata URL.

To fix please check:

- If network connectivity from the Awingu appliance to the Metadata URL is working. Check via the troubleshoot tools if DNS and network ports are open. If needed configure Awingu to use a proxy server (see global connectivity HTTP Proxy) to access a public Metadata URL. If no access is possible to the metadata url you can also upload the XML file directly on the Awingu appliance.
- If the metadata URL is hosted on an internal website and the connection is done over https make sure the certificate is a public certificate, not a private certificate that is only known in the windows environment. If needed you can also move the XML file from the internal website to the awingu appliance by uploading the file.
- In the domains settings of this tenant the correct public host header for the Awingu appliance is set.

Awingu shows an InvalidNameIDPolicy

This error mostly occurs when using Awingu in combination with ADFS.

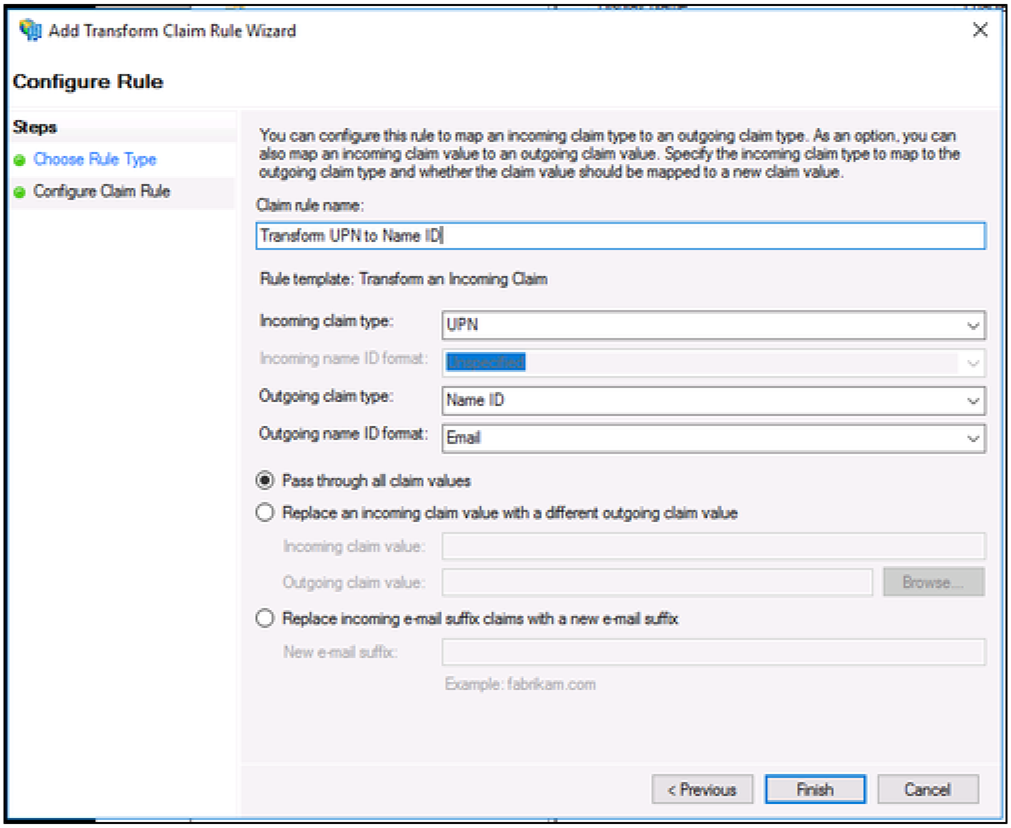
User goes to Awingu, Awingu redirects to the ADFS authentication page, authentication into ADFS is successful but when returning to Awingu you get the following error:

```
{"error": "The status code of the Response was not Success, was Requester -> urn:oasis:names:
tc:SAML:2.0:status:InvalidNameIDPolicy"}
```

The error could mean one of the following:

- NameID claim is missing
- NameID claim is in the wrong format. The format must be "emailaddress"
- NameID claim is empty

Please check that the transform claim is correctly configured on the ADFS side:



Add Transform Claim Rule Wizard

Configure Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Transform UPN to Name ID

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

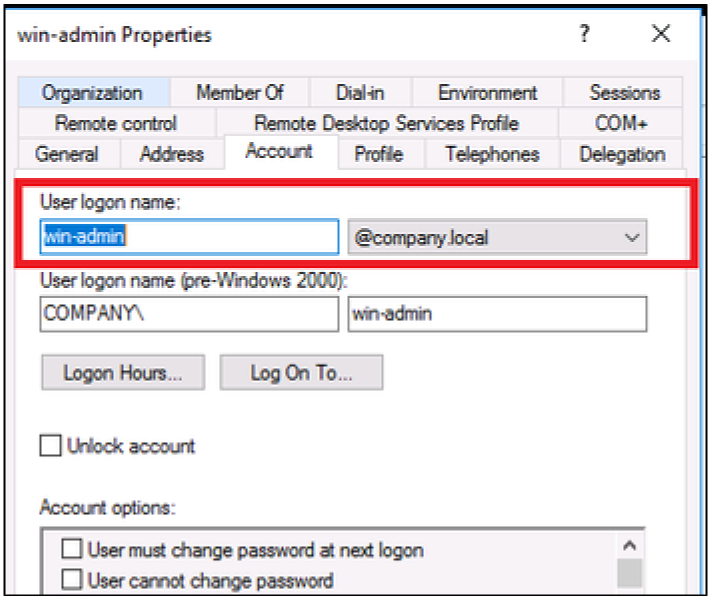
Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Please also check that the accounts you are using have a valid UPN specified:



win-admin Properties

User logon name: win-admin @company.local

User logon name (pre-Windows 2000): COMPANY\ win-admin

□ Unlock account

Account options:

□ User must change password at next logon

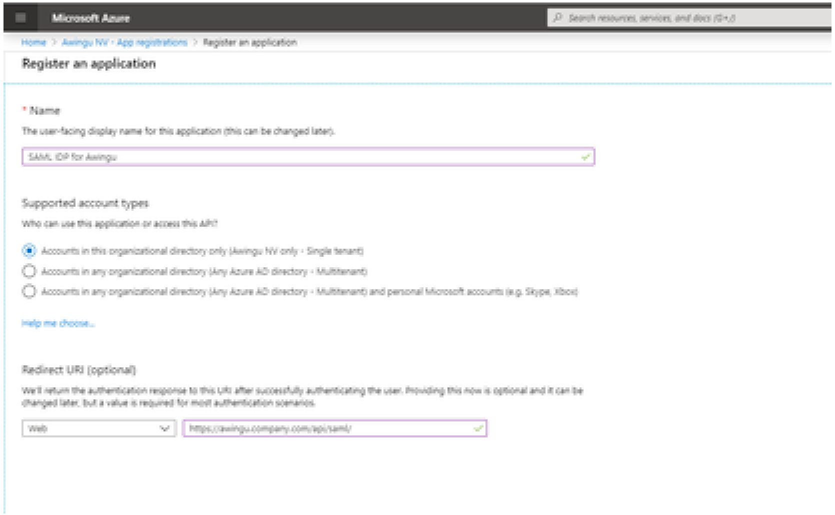
□ User cannot change password

Setting up Azure AD as an external IDP for Awingu

SAML pre-authentication can be configured with Azure AD as the identity provider. The following instructions will show how to configure this in Awingu and in Azure AD.

Register a new Azure Application

1. Login to the Azure Portal
2. Navigate to Azure Active Directory
3. Select from the side bar: *App registrations*
4. Select: *New Registration*
5. Provide a name and supported account type
6. Add redirect URI:
    a. Set the type to Web
    b. Provide the following URL: https://awingu.company.com/api/saml/ where "awingu.company.com" points to your Awingu Environment. (Make sure to add the trailing slash)



Microsoft Azure

Search resources, services, and docs (G+/)

Home > Awingu NV - App registrations > Register an application

Register an application

* Name

The user-facing display name for this application (this can be changed later).

SAML IDP for Awingu ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Awingu NV only - Single tenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

Help me choose...

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://awingu.company.com/api/saml/ ✓

Collect the needed information to complete the setup on the Awingu appliance

There are two properties that we will need from the Azure Application during the configuration in Awingu:

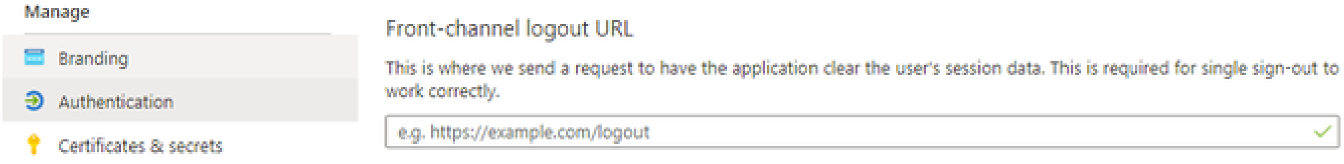
- Application ID (format: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx) which can be found in the properties of the Azure Application on the Overview page of the app.
- Federation metadata document URL (format: https://login.microsoftonline.com/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx /federationmetadata/20-07-06/federationmetadata.xml) which can be found on the dialog that appears when clicking Endpoints on the Overview page of the app.

Configuration for Single Logout

During the configuration of the IdP in the Federated Authentication section of Awingu, the Single Logout feature(SLO) can be enabled. When enabled, the user will also be logged out of the IdP when logging out of Awingu.

The following configuration is required on the IdP:

1. Open the previously created Application in the Azure Portal
2. Click *Authentication* in the left menu
3. Add the Workspace Single Logout URL (shown in the Federated Authentication configuration in Awingu) to the *Front-channel logout URL*



Front-channel logout URL

This is where we send a request to have the application clear the user's session data. This is required for single sign-out to work correctly.

e.g. https://example.com/logout ✓

Note: Only front-channel logout is supported. If the users closes his browser during the logout process, the user might still be logged in to the IdP.

Setting up Azure AD with OPSWAT as external IDPs for Awingu

SAML pre-authentication can be configured with Azure AD as the Primary IDP and OPSWAT as the Intermediate IDP. The following instructions demonstrate how to configure this in Awingu, in Azure AD and OPSWAT.

Register a new Azure Enterprise Application

1. Login to the Azure Portal
2. Navigate to Azure Active Directory
3. Select from the side bar: *Enterprise applications*
4. Click *Add* and *Create your own application*
5. Provide a name and choose *Integrate any other application you don't find in the gallery (Non-gallery)*
6. Collect the needed information by clicking on *Single sign-on* in the left menu and *SAML* as the single sign-on method.
    a. Copy the App Federation Metadata URL(1).
    b. Download the SAML Signing Certificate (Base64)(2).
    c. Copy the Login URL(3).

Configure OPSWAT

1. Login to the OPSWAT MetaAccess console
2. Add Identity Provider:
    a. Navigate to *Secure Access > Access Methods.*
    b. Click the *Identity Providers* tab.
    c. Click the *Create New Identity Provider* button.
    d. Provide a name and upload the previously downloaded SAML Signing Certificate (Base64)(2) from the Azure Enterprise Application.
3. Add Protected App:
    a. Navigate to *Secure Access > Protected Apps.*
    b. Click the *Add Protected Application* button
    c. Select *IdP Method.*
    d. Select the previously created IDP (Choose from existing IDPs).
    e. Fill in the form:
        i. Choose an Application Name.
        ii. Define an Access Mode:
            1. Monitor: Audit logs will be created, access will not be restricted.
            2. Enforced: You will only be able to login if you install the OPSWAT MetaAccess client. You will get a link to download this if you try to login without it being installed.
        iii. IdP Login URL: Provide the previously copied Login URL(3) from the Azure Enterprise Application.
        iv. App ACS URL:
            1. Login to Awingu and Open the System Settings
            2. Navigate to the Configure > User Connector > Federated Authentication section
            3. Select Pre-authentication or Single sign-on as Type (See Enabling Single Sign-On (SSO) for the additional configuration steps to enable Single sign-on).
            4. Select *SAML with Intermediate IdP* as the protocol.
            5. Copy the read-only field *ACS URL* and use this as the App ACS URL in the Protected App form.
        v. Click *Add*
    f. Collect the needed information by opening the newly created Protected App and clicking the *SSO Setup Instructions* tab.
        i. Copy the ACS URL(4).
        ii. Download the Certificate(5).

Update the Azure Enterprise Application

1. Login to the Azure Portal, navigate to the Enterprise Applications and open the recently created Enterprise Application.
2. Click *Single sign-on* in the left menu
3. Click the *Edit* button of the first section (*Basic SAML Configuration)*
    a. Specify an Entity ID(6) and copy this value.
    b. Add the copied ACS URL from OPSWAT as a Reply URL(4).

Enable Pre-authentication with Intermediate IdP in Awingu

1. Login to Awingu and open the System Settings
2. Navigate to the Configure > User Connector > Federated Authentication section
    a. **Entity Id:** Add the copied Entity ID(6) from the step before.
    b. **Metadata Type:** URL
    c. **Metadata URL:** The previously copied Metadata URL (1).
    d. **Intermediate ACS URL:** The previously copied ACS URL from OPSWAT (4)
    e. **Intermediate Signing Certificate:** The previously downloaded certificate from OPSWAT(5).
3. See Enabling Pre-Authentication (PreAuth) for the general configuration.

Setting up ADFS as an external IDP for Awingu

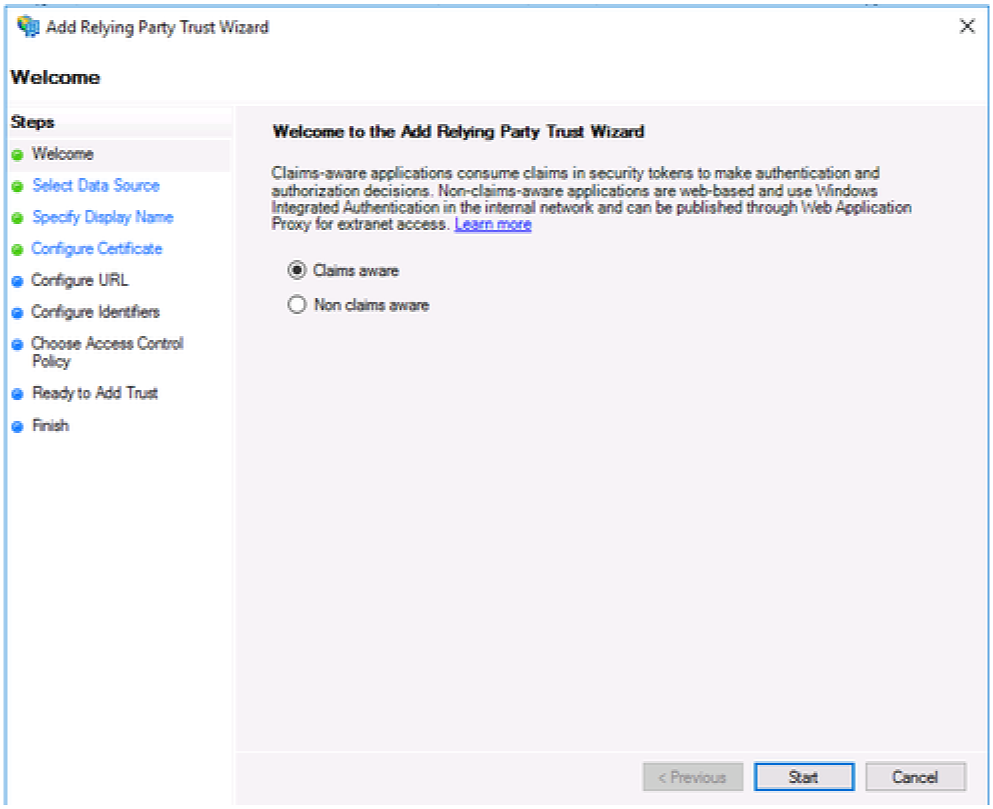
To configure Awingu with ADFS as the external IDP, you first need to add Awingu as a "Relying Party Trust" in ADFS, after this we need to setup the correct claims to be passed to Awingu.

Before you start make sure that you know your Awingu Base URL.

Add Awingu as a relying party trust:

Go to your ADFS host and start the "AD FS Management Tool", select Relaying Party Trusts and right click on it, then open the "Add Relaying Party Trust ..." wizard

On the welcome screen select "claims aware" and click on start



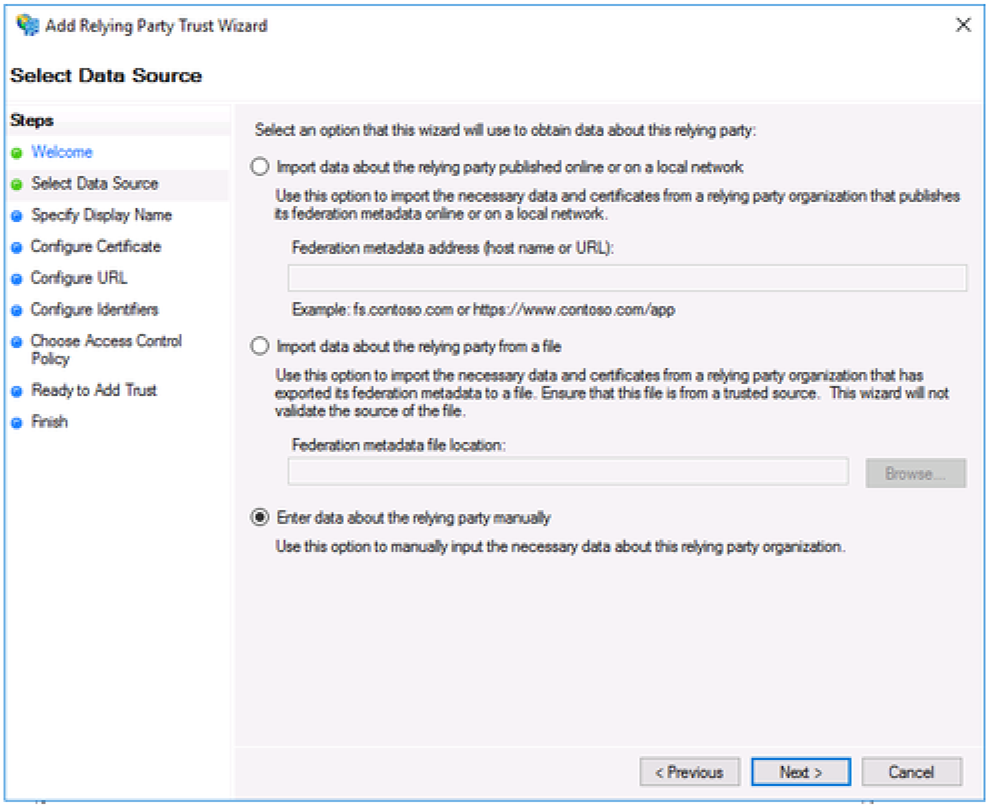
Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware

On the Select Data Source page select "Enter data about the relying party manually"



Select Data Source

Select an option that this wizard will use to obtain data about this relying party:

○ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

○ Import data about the relying party from a file

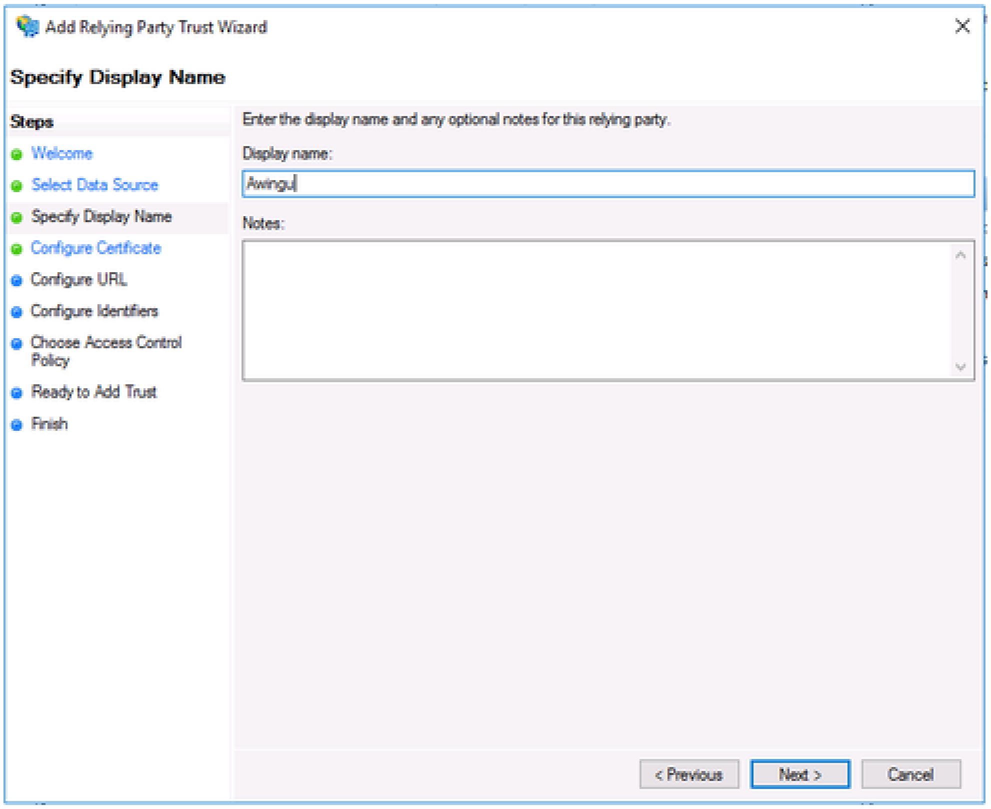
Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

● Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

Select a Display Name. This will be the name that is displayed in the overview of all relying party trusts.



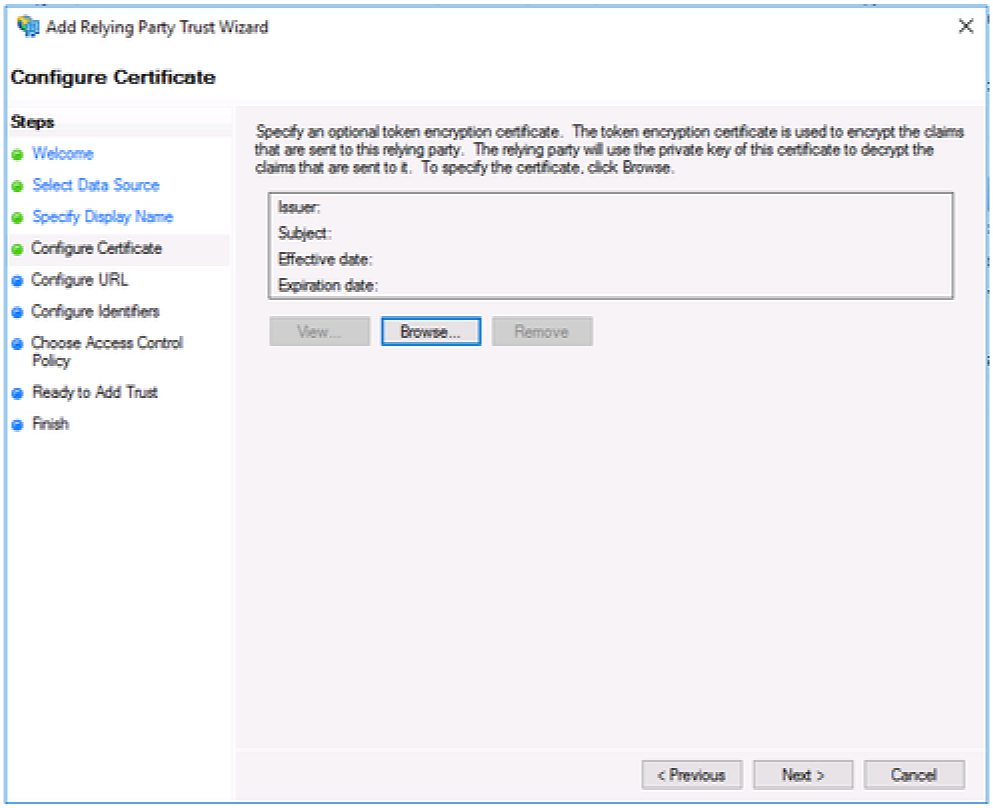
Specify Display Name

Enter the display name and any optional notes for this relying party.

Display name: Awingu

Notes:

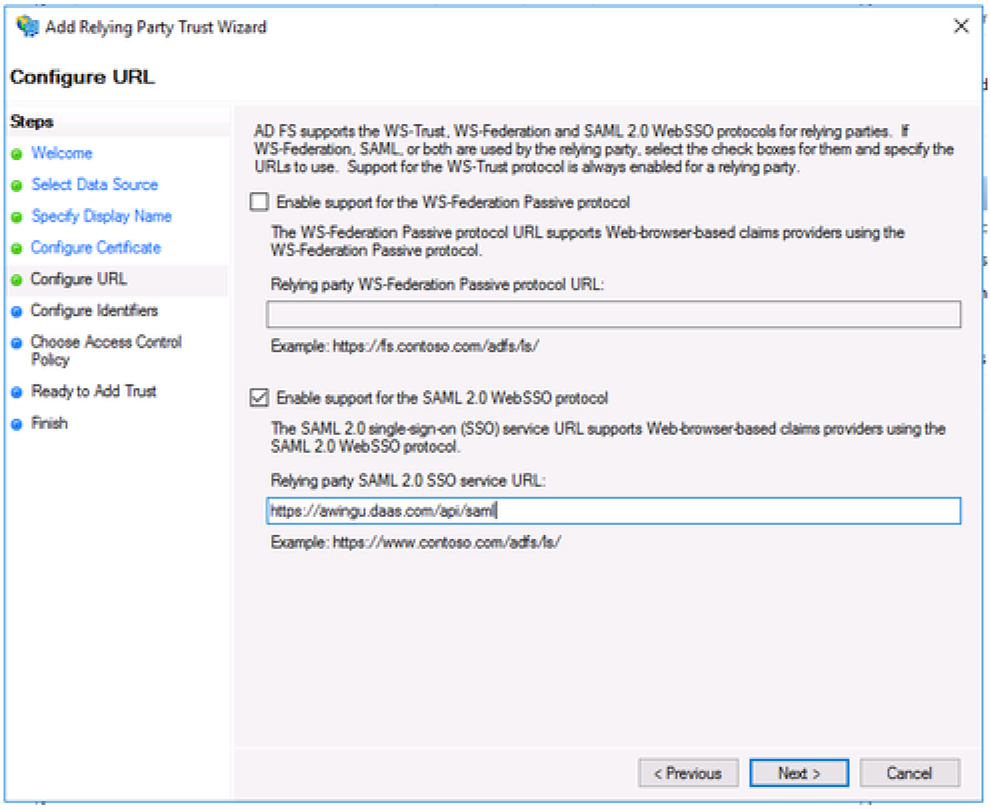
Awingu doesn't need an extra certificate to encrypt the claims. Leave this blank



Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse.

Issuer:
Subject:
Effective date:
Expiration date:

Select the SAML 2.0 WebSSO protocol and set the URL to your Awingu SAML URL. The URL can be found in the pre-authentication configuration in Awingu System Settings, but is typically your Awingu base URL + /api/saml. So for example https://awingu.company.com/api/saml



AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

□ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☑ Enable support for the SAML 2.0 WebSSO protocol

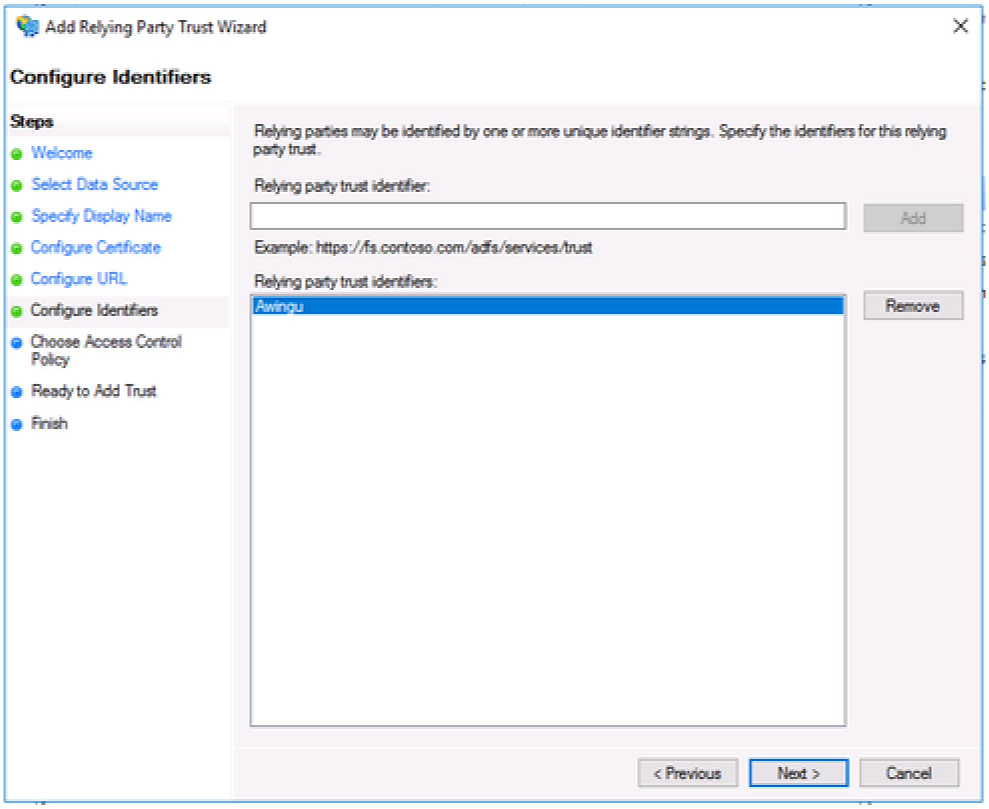
The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://awingu.daas.com/api/saml

Example: https://www.contoso.com/adfs/ls/

This field should correspond to the "identity ID" specified in the Awingu pre-authentication configuration.



Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

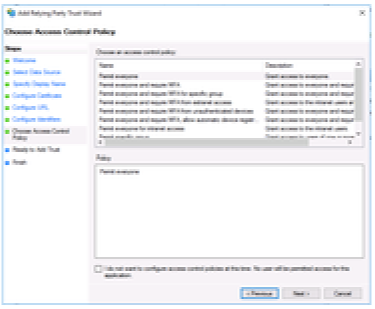
Relying party trust identifier:

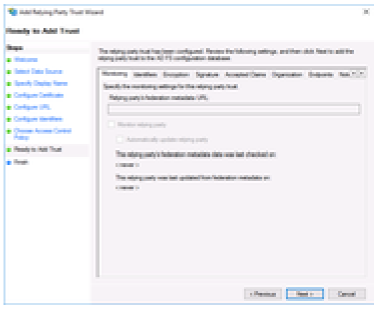
Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

Awingu

The rest of the configuration can be done with default settings, no changes needed:





Add the necessary Awingu claims

Once the "Trusted Relying Party" is create you can add claims by selecting the relying party trust and then in the actions menu choose the "Edit Claim Issuance Policy ..."

First - We will select the AD attributes that will be sent as claims to Awingu.

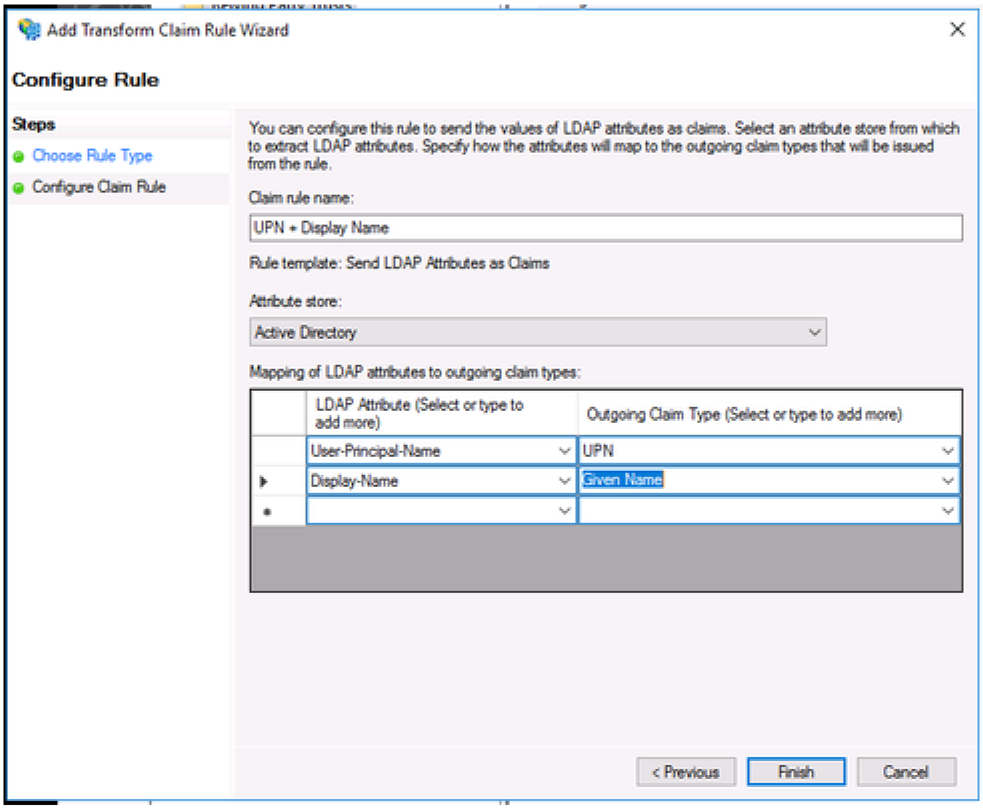
Add a rule based on the "Send LDAP Attributes as Claims" template:

Set the Attribute store to: Active Directory

Add 2 Claims:

- User-Principle Name UPN
- Display-Name Given Name

In this case User-Principle Name and Display-Name will be sent to Awingu.



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: UPN + Display Name

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

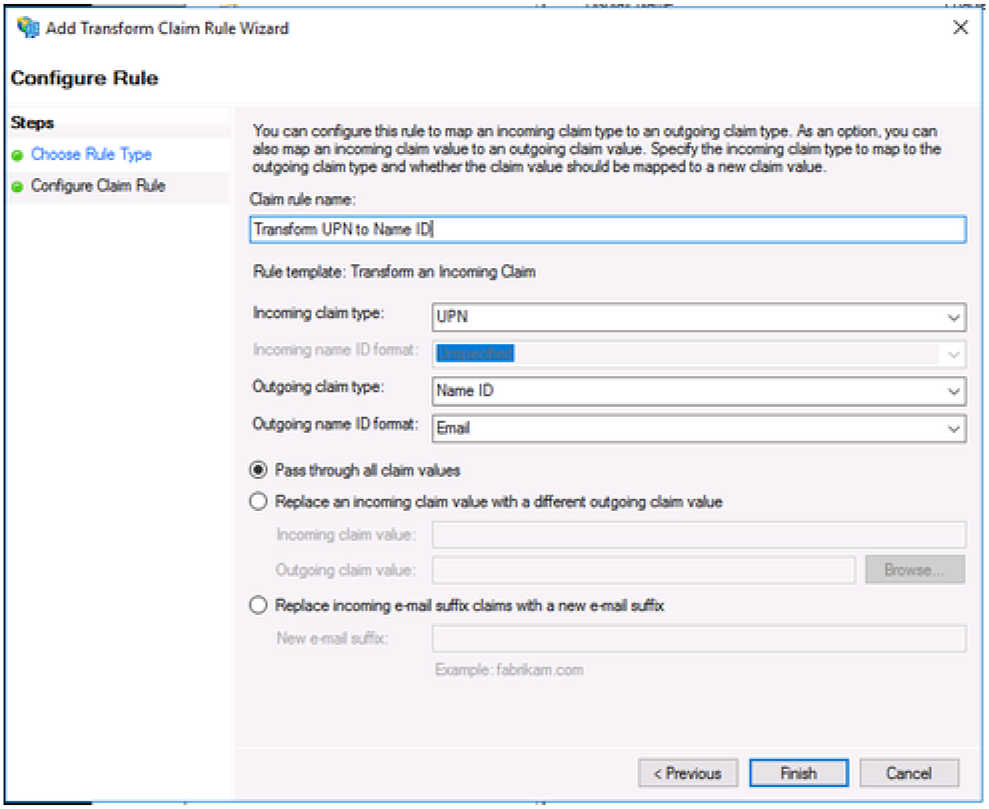
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	User-Principal-Name	UPN
▶	Display-Name	Given Name
*		

Second - We will add the mandatory Name ID claim.

Add a rule based on the "Transform an Incoming Claim" template:

As the name ID field is a mandatory field in the ADFS setup and the format must be Email, we need to add a transform rule that sets the Name ID field based on the existing UPN.



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name: Transform UPN to Name ID

Rule template: Transform an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Email

● Pass through all claim values

○ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

○ Replace incoming e-mail suffix claims with a new e-mail suffix

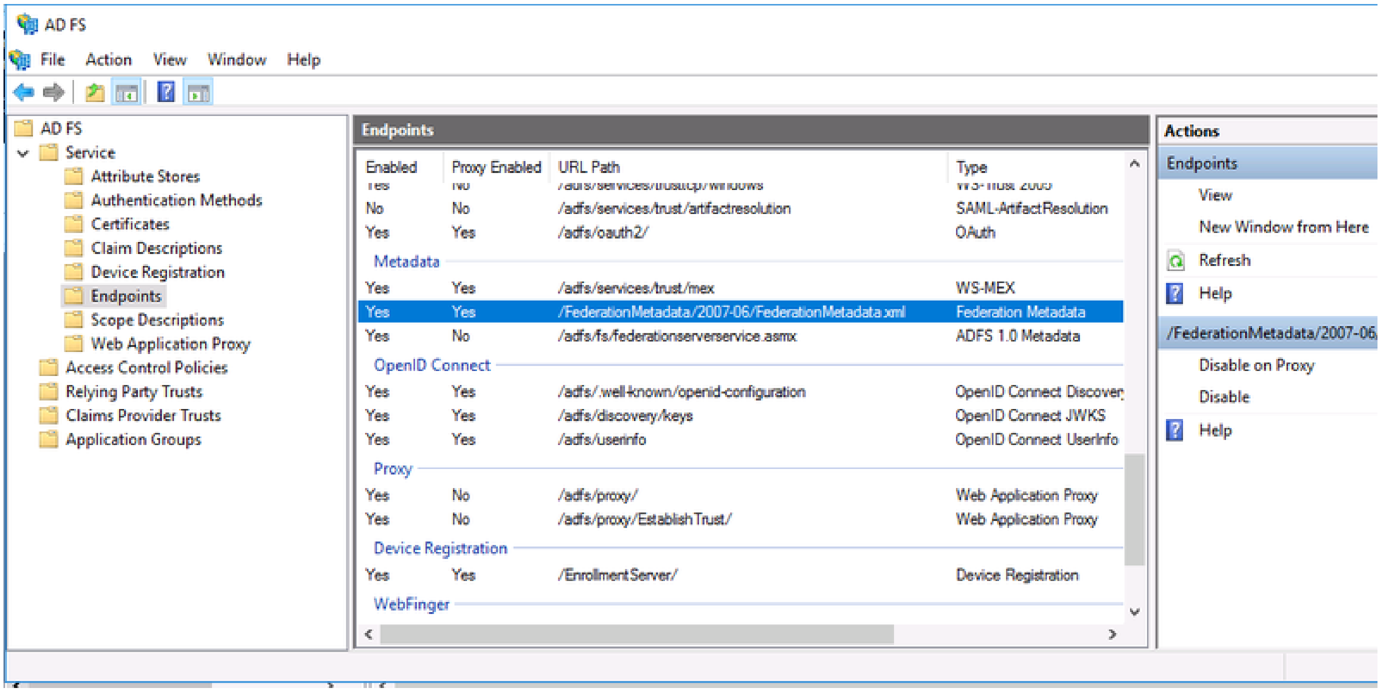
New e-mail suffix:

Example: fabrikam.com

Collect the needed information to complete the setup on the Awingu appliance

There are two properties that we will need from the Azure Application during the configuration in Awingu:

- Relying Party Trust Identifier. This is the value chosen during the wizard setup of the relying party trust. This will correspond with the Entity ID configuration in Awingu
- Federation metadata. This can be found in the AD FS management tool under Service Endpoints Metadata Federation Metadata

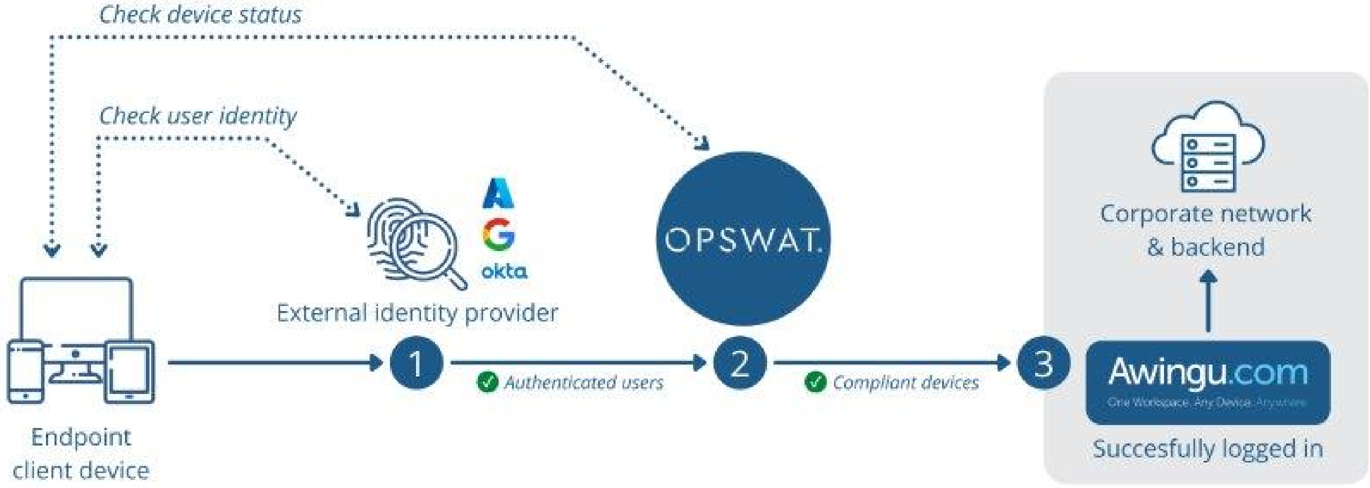


Enabled	Proxy Enabled	URL Path	Type
Yes	No	/adfs/services/trusttcp/windows	WS-Trust 2005
No	No	/adfs/services/trust/artifactresolution	SAML-ArtifactResolution
Yes	Yes	/adfs/oauth2/	OAuth
Metadata			
Yes	Yes	/adfs/services/trust/mex	WS-MEX
Yes	Yes	/FederationMetadata/2007-06/FederationMetadata.xml	Federation Metadata
Yes	No	/adfs/fs/federationserverservice.asmx	ADFS 1.0 Metadata
OpenID Connect			
Yes	Yes	/adfs/.well-known/openid-configuration	OpenID Connect Discover
Yes	Yes	/adfs/discovery/keys	OpenID Connect JWKS
Yes	Yes	/adfs/userinfo	OpenID Connect UserInfo
Proxy			
Yes	No	/adfs/proxy/	Web Application Proxy
Yes	No	/adfs/proxy/EstablishTrust/	Web Application Proxy
Device Registration			
Yes	Yes	/EnrollmentServer/	Device Registration
WebFinger			

Setting up ADFS with OPSWAT as external IDPs for Awingu

Next to setting up Awingu with a single IDP like ADFS. It is also possible to setup Awingu in combination with multiple, chained, IDP’s.

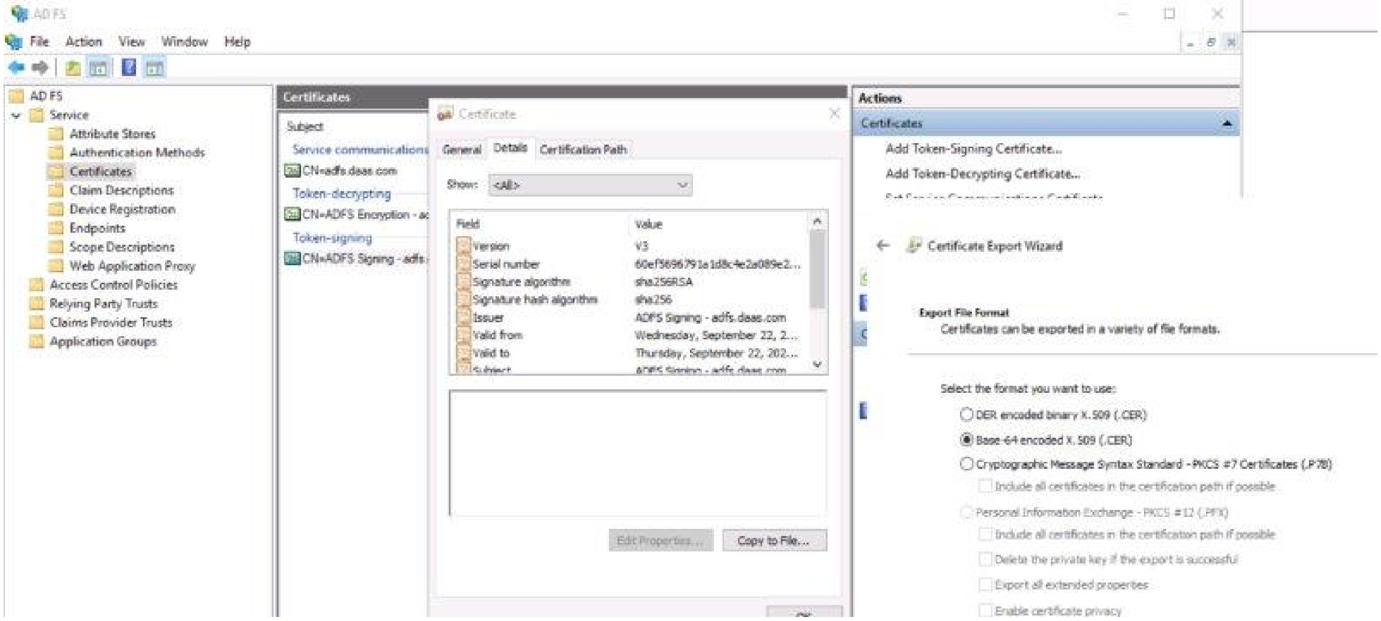
In this case we are going to configure Awingu in combination with ADFS for the user validation part and then with OPSWAT to validate the device. For more information on OPSWAT have a look at https://docs.opswat.com/macloud-sdp



Before you start with this setup please make sure that first Awingu in combination with ADFS is working. If this is working we can then extend the setup to add OPSWAT into the configuration. See Setting up ADFS as an external IDP for Awingu for instructions on this.

Step 1: Export the token-signing certificate from your ADFS

Login to the ADFS configuration panel, goto Services Certificates and select the “Token-signing” certificate. Under details you will see an option to “copy to File” and export the certificate in a “Base-64 encoded” format.



Field	Value
Version	V3
Serial number	60ef5696791a1d8c4e2a089e2...
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	ADFS Signing - adfs.daas.com
Valid from	Wednesday, September 22, 2...
Valid to	Thursday, September 22, 202...
Subject	ADFS Signing - adfs.daas.com

Export File Format
Certificates can be exported in a variety of file formats.

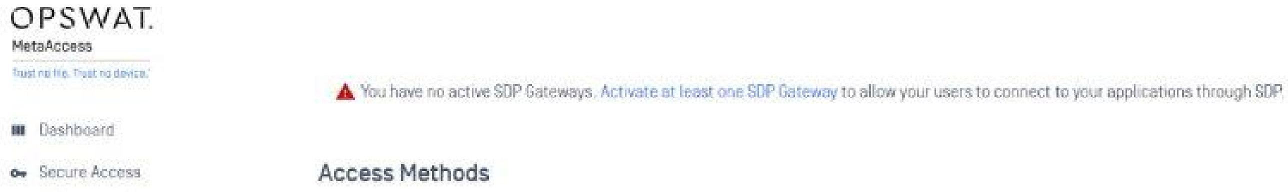
Select the format you want to use:

○ DER encoded binary X.509 (.CER)
● Base-64 encoded X.509 (.CER)
○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
□ Include all certificates in the certification path if possible
○ Personal Information Exchange - PKCS #12 (.PFX)
□ Include all certificates in the certification path if possible
□ Delete the private key if the export is successful
□ Export all extended properties
□ Enable certificate privacy

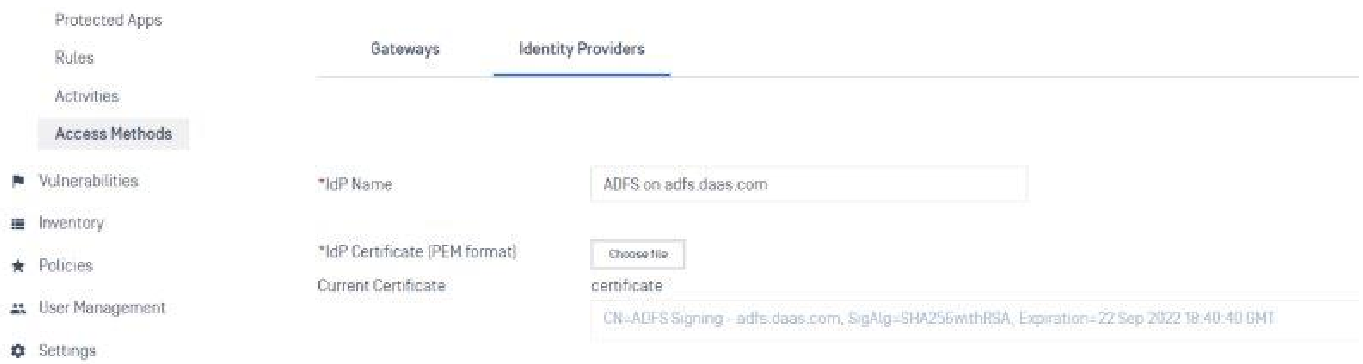
Step 2: Configure OPSWAT

If not yet done add your ADFS as an “Identity Provider”: Login to your OPSWAT console and under “Secure Access” “Access Methodes” add select “Create New Identity Provider”.

When asked for the IdP Certificate upload the ADFS certificate downloaded in the previous step.



You have no active SDP Gateways. Activate at least one SDP Gateway to allow your users to connect to your applications through SDP.



*IdP Name: ADFS on adfs.daas.com

*IdP Certificate (PEM format)

Current Certificate: certificate

CN=ADFS Signing - adfs.daas.com, SigAlg=SHA256withRSA, Expiration=22 Sep 2022 18:40:40 GMT

Now add in OPSWAT a new protected application:

Select “Secure Access” “Protected Apps” “Add Protected App”.

When asked for the methode select: “IDP Setup” and select in the dropdown list your ADFS IDP you have added in the step before.

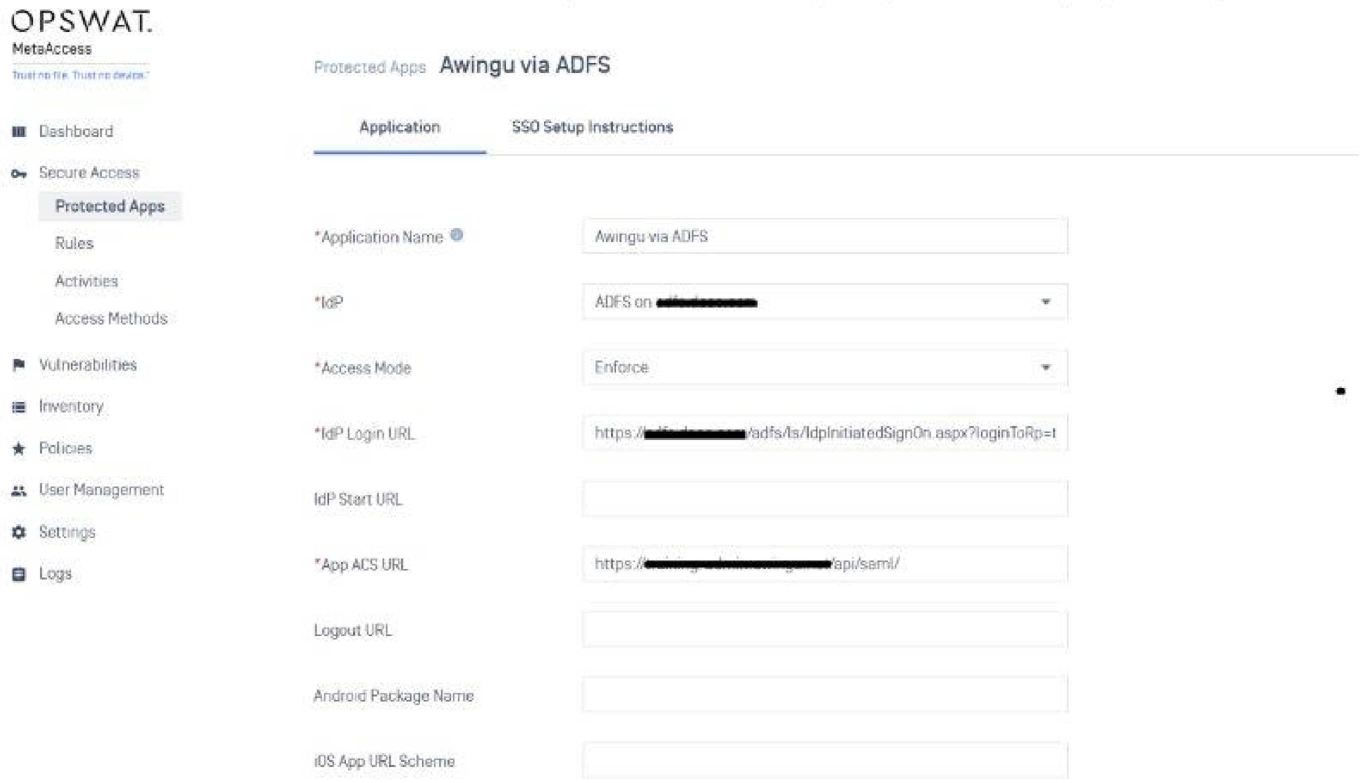
Use following parameters:

- *Application Name:* Free text.
- *IDP:* if not yet done select the ADFS IDP added in the step before
- *Access Methode:*
  - select Enforce if you want to make sure only trusted devices can login
  - select Monitor if you want to only log the connections from non-trusted devices
- *IdP login URL:* Set this value to https://<your.adfs.url>/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=<RelayingPartyTrust>

RelayingPartyTrust can be found on the ADFS configuration and is the identifier of this ADFS Relaying Party Trust. So for example set the URL to : https://adfs.mycompany.com/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=awingu

- *App ACS URL:* Set this to the value you can find in Awingu under “configure” “user connector” “federated authentication” “ACS URL

In most cases this will be something like https://<your.awingu.ul>/api/saml/



Awingu via ADFS

*Application Name: Awingu via ADFS

*IdP: ADFS on [redacted]

*Access Mode: Enforce

*IdP Login URL: https://[redacted]/adfs/ls/IdpInitiatedSignOn.aspx?loginToRp=t

IdP Start URL

*App ACS URL: https://[redacted]/api/saml/

Logout URL

Android Package Name

iOS App URL Scheme

Once the application is added you will get 2 sets of information back from OPSWAT:

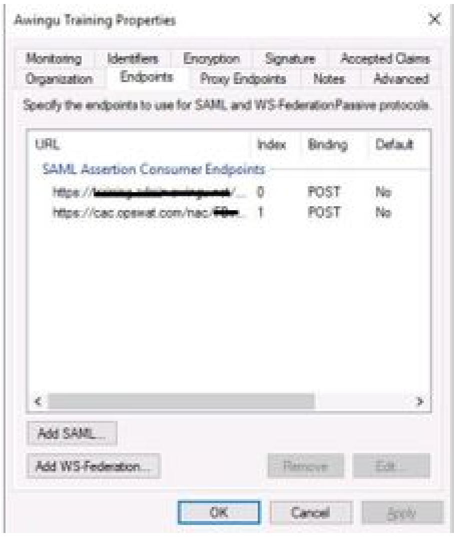
1. An ACS URL that needs to be added to the Identity provider. The URL looks like https://cac.opswat.com/nac/XXXXXXXXX/check/<your_app>
2. An OPSWAT Certificate. Download the certificate to your local computer

Step 3: Add the OPSWAT ACS URL to ADFS

Go back to the ADFS configuration and rightclick on the relying party trust and select “properties”.

Goto the “Endpoints” tab and click on “Add SAML”

Select “Endpoint Type”: SAML Assertion Consumer & “Binding”: POST
Set the Index to 1
Set the Trusted URL to the ACS URL received when creating the OPSWAT protected app (https://cac.opswat.com/nac/XXXXXXXXX/check/<your_app>)



Awingu Training Properties

Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default
SAML Assertion Consumer Endpoints			
https://[redacted]/...	0	POST	No
https://cac.opswat.com/nac/[redacted]...	1	POST	No

Step 4: Configure Awingu

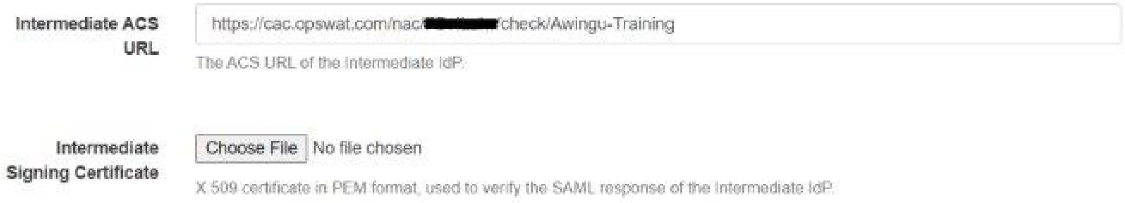
Last thing to do now is to modify the existing ADFS SAML configuration on Awingu from simple “SAML” to “SAML with intermediate IDP”

Goto the Awingu system settings Configure User Connector Federated Authentication.

Select from the “protocol” dropdown list “SAML with Intermediate IDP”.

You will notice that 2 extra fields become visible:

- Intermediate ACS URL: Set this to the same ACS URL received when creating the OPSWAT protected app (same as the one added in the step before in ADFS).
- Intermediate Signing Certificate: upload the certificate you received when creating the OPSWAT protected app.



Intermediate ACS URL: https://cac.opswat.com/nac/[redacted]check/Awingu-Training

The ACS URL of the intermediate IdP.

Intermediate Signing Certificate: Choose File No file chosen

X.509 certificate in PEM format, used to verify the SAML response of the intermediate IdP.

Check if all fields that were previously filled in with the standard ADFS settings are still filled in as before and if so click on “Apply”.

Step 5: Test if it works

Now open an in-private browser window. Go to the Awingu URL

If things are correct configured you should be redirected to ADFS.

After successful login ADFS will send you to OPSWAT.

After successful device validation in case of “enforced” mode you will be redirected to Awingu. In case of “monitor” mode you will see for a few seconds OPSWAT spinner and then arrive on Awingu.

If in Awingu the federated authentication is set to Single sign-on you will arrive directly in the workspace. If it is set to pre-authentication you will have to provide your windows password to get in.

Setting up Google as an external IDP for Awingu

OpenID Connect pre-authentication can be configured with Google as the identity provider. The following instructions will show how to configure this in Awingu and in Google.

Register a new

1. Login to the Google Developers console and go to the credentials API page: https://console.developers.google.com/apis/credentialsf
2. First we need to add the domain on which Awingu is hosted is to the list of Authorized Domains
   Select *OAuth consent screen Authorized Domains*
   Add your domain to the list of authorized domains. (for example if your awingu is hosted on awingu.company.com, add company.com to the list)

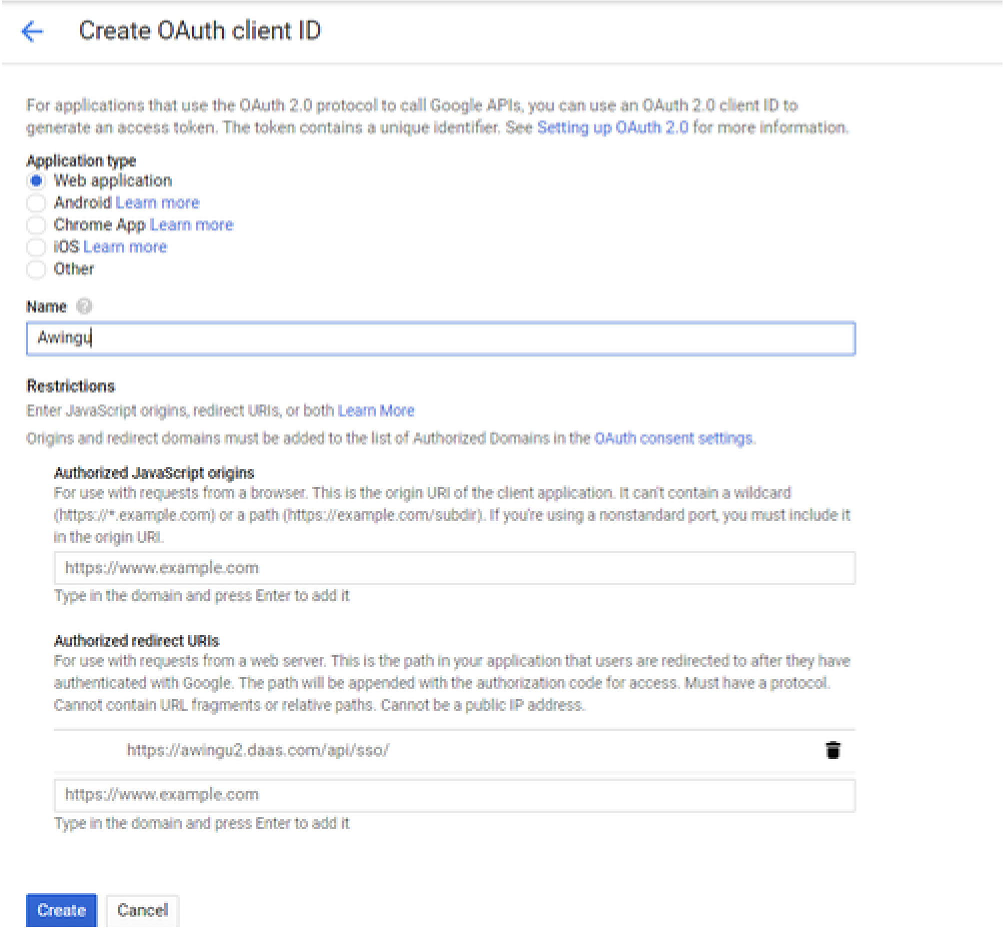
   Click on **Save** at the bottom of the page.

   See https://support.google.com/cloud/answer/6158849?hl=en&authuser=2#authorized-domains for more details

3. Now we can add Awingu as an OpenID Connect client in Awingu
   Select *Create Credentials OAuth Client ID*

   Application Type: Web application
   Name: Display name of these credentials in the Google Developers console
   Authorized Redirection URLS: https://awingu.company.com/api/sso/ where "awingu.company.com" points to your Awingu Environment. (Make sure to add the trailing slash)

   Click on **Save** at the bottom of the page.



Create OAuth client ID

For applications that use the OAuth 2.0 protocol to call Google APIs, you can use an OAuth 2.0 client ID to generate an access token. The token contains a unique identifier. See Setting up OAuth 2.0 for more information.

Application type
● Web application
○ Android Learn more
○ Chrome App Learn more
○ iOS Learn more
○ Other

Name
Awingu

Restrictions
Enter JavaScript origins, redirect URIs, or both Learn More
Origins and redirect domains must be added to the list of Authorized Domains in the OAuth consent settings.

Authorized JavaScript origins
For use with requests from a browser. This is the origin URI of the client application. It can't contain a wildcard (https://*.example.com) or a path (https://example.com/subdir). If you're using a nonstandard port, you must include it in the origin URI.
https://www.example.com
Type in the domain and press Enter to add it

Authorized redirect URIs
For use with requests from a web server. This is the path in your application that users are redirected to after they have authenticated with Google. The path will be appended with the authorization code for access. Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.
https://awingu2.daas.com/api/sso/
https://www.example.com
Type in the domain and press Enter to add it

   See https://developers.google.com/identity/protocols/OAuth2 for more details

Collect the needed information to complete the setup on the Awingu appliance

There are 3 properties that we will need from the Azure Application during the configuration in Awingu:

- **Client ID** and **Secret** are provided by the Google API after finishing the above setup.
- The **Discovery URL** for Google is:

  ```
  https://accounts.google.com/.well-known/openid-configuration
  ```

Enabling Single Sign-On (SSO)

Before enabling Single Sign-On (SSO) first make sure that the **pre-authentication is working** with your external identity provider (IDP).

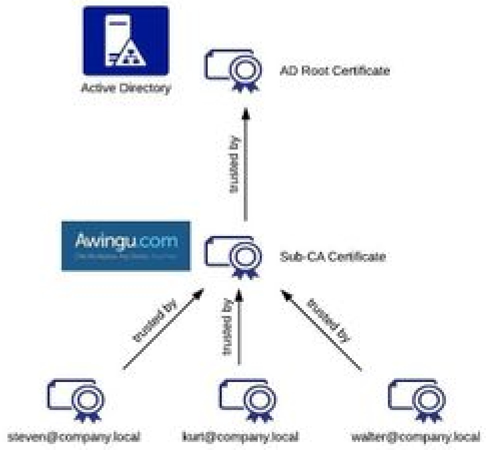
See "Enable Pre-Authentication" for detailed instructions on how to do this.

By enabling SSO in Awingu we will remove the step where the user is prompted for the windows password, prior to opening the Awingu workspace. To get this working Awingu will need a trusted X.509 client certificate so it can log users into applications, virtual desktops and drives.

The certificate will be used to:

1. Generate a Kerberos ticket to
   a. Login to the windows network (NLA)
   b. Access the CIFS drives
2. Generate a virtual smart-card to allow RDP login (win-logon)

To get this working the Awingu appliance will act as a sub-certificate (sub-CA) authority and will automatically generate & manage those client certificates. In order to be able to generate those certificates, Awingu requires an AD signed certificate and private key that is trusted by all Windows servers that require Awingu SSO access.



Generate Certificate & Setup the intermediate Sub-CA

Create the certificate

On the windows Domain Controller, create the "awingu.inf" certificate template with the following content. This can be done in notepad or any other text editor.

```
[NewRequest]
Subject = "CN=AwinguCA"
KeyLength = 4096

[RequestAttributes]
CertificateTemplate= SubCA
```

Use "certreq" to request certificates from the certification authority (CA).

```
certreq.exe -new awingu.inf awingu.req
certreq -submit awingu.req awingu.cer
```

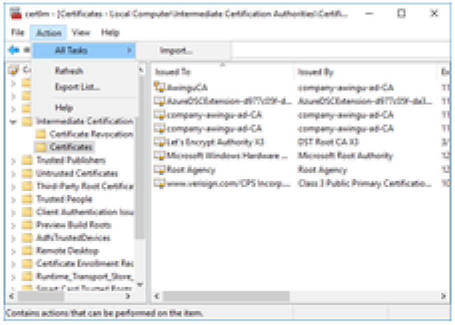
See https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/certreq_1 for more details.

Import the certificate into the needed certificate stores

In the next step we will import the certificate into the AD certificate store;

Run certlm.msc and import the certificate:

- Select the intermediate certificate store certificates
- Go to Actions All Tasks Import
- Run through the wizard and import the awingu.cer file



Issued To	Issued By
AwinguCA	company-awingu-ad-CA
AzureDSCExtension-d977c09f-d...	AzureDSCExtension-d977c09f-da3...
company-awingu-ad-CA	company-awingu-ad-CA
company-awingu-ad-CA	company-awingu-ad-CA
Let's Encrypt Authority X3	DST Root CA X3
Microsoft Windows Hardware ...	Microsoft Root Authority
Root Agency	Root Agency
www.verisign.com/CPS Incorp...	Class 3 Public Primary Certificatio...

Contains actions that can be performed on the item.

Once this is done we still need to configure the AD to allow smart card logins that are signed with this intermediate certificate. As these client certificates will be generated by the Awingu CA (and as such be signed with this intermediate certificate), the Intermediate Certificate needs to be added to NTAuthStore of the AD:

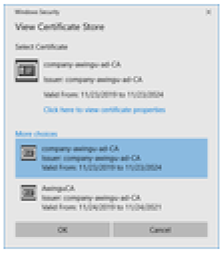
```
certutil -dspublish -f awingu.cer NTAuthCA
certutil -enterprise -addstore NTAuth awingu.cer
```

See https://support.microsoft.com/en-us/help/295663/how-to-import-third-party-certification-authority-ca-certificates-into for more information.

You can check if the import was successful by running the following command:

```
certutil -enterprise -viewstore NTAuth
```

Both the AD root certificate and the intermediate Awingu certificate should be visible. Click on "more choices" to see all certificates



View Certificate Store

Select Certificate

company-awingu-ad-CA
Issuer: company-awingu-ad-CA
Valid From: 11/23/2019 to 11/23/2024

company-awingu-ad-CA
Issuer: company-awingu-ad-CA
Valid From: 11/23/2019 to 11/23/2024

AwinguCA
Issuer: company-awingu-ad-CA
Valid From: 11/24/2019 to 11/24/2021

Export Certificates & private key

To enable SSO in Awingu 2 files are needed:

1. The Intermediate Certificate in pfx format, including the private key.
2. The root Certificate of the AD in cer format. This is needed to complete the certificate chain trust

Export the intermediate Certificate (with private key) in pfx format:

To get the root certificate we need to open certlm.msc again:

- Select the *Intermediate Certification Authorities* store certificates
- Right click on the subca certifcate (in this case AwinguCA) and select All tasks export
- The export wizard will start

  - select “yes export the private key” on the second page
  - select “Personal Information Exchange - PKCS # 12 (.PFX) as format. Leave default settings (“include all certificates in the certificatin path if possible” + “enable certificate privacy”)
  - set a password on the certificate
  - Finally on the "File to Export" page set the output file to subca.pfx
  - Finish the wizard

Export Root Certificate (without private key)

To get the root certificate we need to open certlm.msc again:

- Select the *Trusted Root Certification Authorities* store certificates
- Right click on the root certificate of your AD and select All tasks Export (in case you don't know what the root certificate of your AD is, open the intermediate certificate first and check the certification path. The certificate that has signed the intermediate certificate is the certificate that is needed)
- The export wizard will start
  - On the "Export File Format" page select "Base 64 encoded X.509 (.cer)"
  - Finally on the "File to Export" page set the output file to root*.cer*
  - Finish the wizard

Important if there is more than only the root certificate used in the certification path of the Awingu Sub-CA then also the other certificates in the certificate chain need to be extracted in the same way as documented above for the root certificate and need to be stored in a single file (copy the content of the different cer files into a single file). To be clear assume that your Awingu SUB-CA is signed by another intermediate certificate and then this intermediate certificate signed by the root certificate then both this other intermediate certificate and the root certificate need to be extracted and the result of both need to be merged into a single root.cer file.

Validate if the Windows back-end is correctly configured for Awingu SSO

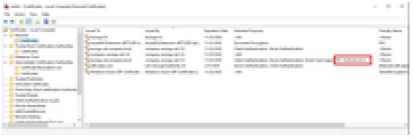
Validate the Kerberos Certificates

Awingu SSO is partly based on Kerberos Constraint Delegation (KCD). To have this working the Kerberos setup needs to be done correctly.

If this is the first time KCD is used on this windows back-end there is a possibility that there is not yet a Kerberos Certificate.

To check if there is a (valid) Kerberos certificate open the cerlm.msc again:

- Select the *Personal* store certificates
- Check if one of the AD certificates (certificates with the name of the Domain Controller) has a certificate with "Intended Purposes" set to "KDC Authentication"



If there is no valid certificate add one first:

- Go to Personal Certificates
- Right click on Certificates All tasks Request New Certificate
- Click next until you reach what kind of template to use, then select Kerberos

Check your DNS setup.

As Kerberos is highly dependent on DNS, DNS also needs to be configured correctly. In order for Awingu SSO to work, all of the DNS records for the servers defined in the drives, app servers and AD/LDAP server sections of the Awingu configuration need to be accessible with a reverse DNS lookup of its IP.

To check if this is the case do a DNS lookup of the DNS names used in Awingu for AD and other servers and check if the reverse lookup of the IP matches that name:

```
C:\Users\win-admin>nslookup awingu-ad.company.local
Name: awingu-ad.company.local
Address: 10.7.0.4
```

```
C:\Users\win-admin>nslookup 10.7.0.4
Name: awingu-ad.company.local
Address: 10.7.0.4
```

Important is that for reverse lookups of IP addresses Awingu uses the global DNS server. So not the DNS servers of the individual tenants. If you have a multi tenant setup with different DNS settings for the global appliance and for the individual tenants please validate on the Awingu appliance itself if the resolution of the reverse lookup is done correct for the tenants on which you want to enable SSO. This can be done via the troubleshoot page (“global” “troubleshoot”) and then go for “dig”. In the “argument” field set “-x your.ip” (for example -x 10.1.2.3). In the responds. If resolution is done correct in the answer section you should see something similar like:

```
;; ANSWER SECTION:
3.2.1.10.in-addr.arpa. 3600        IN        PTR        server.company.
local
```

Also check if the kerberos SRV records exist for your domain and that they point to the correct KDC. Check both the UDP & TCP records

```
C:\Users\win-admin>nslookup
> set type=srv
> _kerberos._udp.company.local


_kerberos._udp.company.local SRV service location:
                   priority = 0
                       weight = 100
                        port = 88
                        svr hostname = awingu-ad.company.local
awingu-ad.company.local internet address = 10.7.0.4


> _kerberos._tcp.company.local


_kerberos._tcp.company.local SRV service location:
                        priority = 0
                        weight = 100
                        port = 88
                        svr hostname = awingu-ad.company.local
awingu-ad.company.local internet address = 10.7.0.4
```

Update the DNS records where needed (reverse lookup + SRV records) to ensure this is working correctly before continuing.

Make sure all servers involved in Kerberos Authentication can access the Certificate Revocation List

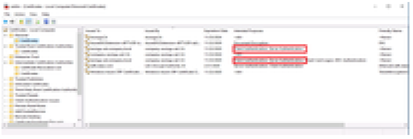
HTTP(s): TCP port 80/443 connectivity from the Active Directory and Application Servers to the Awingu appliance (http(s)://<AWINGU_URL>/crl/>AWINGU_DOMAIN_NAME>) is required.

Make sure LDAPs is enabled on your AD

Similarly to Kerberos, for doing an LDAPs connection a valid Certificate is needed on the AD:

To check if there is at least one (valid) Domain Controller certificate open the cerlm.msc again:

- Select the *Personal* store certificates
- Check if one of the AD certificates (certificates with the name of the Domain Controller) has a certificate with "Intended Purposes" set to "Client Authentication" and "Server Authentication"

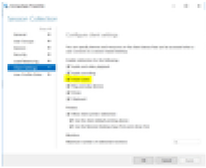


For more information on how to set this up take a look at our support portal: https://support.awingu.com/en/support/solutions/articles/8000055177-tutorial-00-enable-active-directory-over-ssl

Make sure your Connection Broker Session Collection is configured for smart cards

If you are using an RDS Connection Broker Session Collection, then the session needs to have smart card redirection enabled from the client device:

- Open server manager and go to the RDS Session Collection
- Next to "Properties" in the RDS collection Tasks Edit Properties Client Settings Ensure "Smart cards" is ticked under "Enable redirection for the following:"



Configure Awingu for SSO

> Only if;
>
> 1. The sub-CA certificates have been created (root.cer, awingu.cer and awingu.key)
> 2. All dependencies on the windows back-end have been setup (import of the sub-CA certificate in the correct stores, Kerberos & DNS setup correct, etc.)
> 3. Pre-authentication with your external IDP has been configured and tested (see Enable Pre-authentication)
>
> Awingu SSO can then be enabled

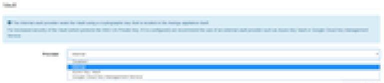
Enable the Awingu Key Vault

Since the private key for the Awingu Sub-CA allows Awingu to impersonate Windows users, this key is highly sensitive and is stored in a vault inside of Awingu. The vault itself is also encrypted and the encryption key for the vault can either be stored on the Awingu appliance itself (Internally) or on an external Vault provider like Google Cloud Key Management Service or Azure Key Vault.

By default the Vault is not activated and needs to be enabled first:

- Open the System Settings and go to *Global Connectivity Vault*
- Select the provider of choice
- Click on Apply.

Enabling the vault might take a few minutes.



For more information on the external Vault providers and how to obtain the needed configuration parameters have a look at:

- Azure Key Vault: https://docs.microsoft.com/en-us/azure/key-vault/key-vault-overview
- Google Cloud Key Management Service: https://cloud.google.com/kms/docs/quickstart

> The private key itself does not leave the vault. After the initial upload it only exists in unencrypted form in the memory of the vault service.

If the Awingu appliance running the vault services is rebooted, access to an external vault provider such as Google GCKMS or Azure Key Vault is required to unseal the vault and decrypt the private key.

Since the vault does not allow extracting the private key, certain configuration changes of the Awingu environment result in a full vault reset, which will disable SSO and require you to re-upload the private key of the CA.

These are:

- Restoring a database backup (only applicable if using Awingu with an internal database)
- Changing the vault provider

For HA purposes, the vault service is replicated across all back-end nodes in an Awingu environment.

If not yet done, set the domain parameters correctly:

When adding a domain to Awingu one of the parameters is specifying if the LDAP connection is over SSL or not.

If this has not yet been done make sure this is enabled;

- Open the System Settings and go to *Global Domains*
- Click on the "edit" button next to the domain you want to check.
- In the *domain details* check if *LDAP over SSL* is set to **enabled**

Also make sure that:

1. The FQDN of the domain is set to the Kerberos realm of the Windows Domain (example: company.local)
2. The AD/LDAP server is set to the correct FQDN of the domain controller. Awingu won't work if the IP address or an alias is used. (example: ad1.company.local)

If not yet done, make sure Awingu is using the correct DNS server

Awingu has DNS servers on 2 levels. One for the appliance itself and one for the tenants/domains.

As the Global DNS server is used for reverse DNS resolution make sure that the Global DNS server is pointing to a DNS server that is capable of resolving all reverse DNS lookups for all tenants/domains using SSO.

To check and modify the global DNS server:

- Open the System Settings and go to *Global Connectivity Servers*
- Set the *DNS IP Addresses* to the correct DNS Server

If not yet done, set Authentication Protocol of Application servers to Kerberos

When adding an application server, the default Authentication Protocol that is used is NTLM. For SSO to work Awingu needs to use Kerberos.

To switch application servers from NTLM to Kerberos

- Open the Awingu System Settings and go to Manage *Application Servers*
- Switch the Authentication Protocol from NTLM to Kerberos
- Make sure the *Authentication Host* is set to the FQDN of the server and that the name specified in here matches the DNS and reverse DNS name

Make sure you set this value for all application servers that Awingu uses with SSO.

Upgrade from Pre-Authentication to Single Sign-On:

Now that all settings both on the windows back-end and the Awingu appliance are set, we can update the configuration to switch from Pre-Authentication to SSO

- Open the System Settings and go to *Configure User Connector Federated Authentication*
- Change the Type from *Pre-Authentication to* Single sign-on
- You will notice that below the existing Pre-Authentication configuration 2 extra certificate settings will appear: *CA Certificate* and *CA Trusted Roots File*

- Select *Manual PKCS 12* as the type for CA Certificate and upload the “subca.pfx” file + set the CA certificate password to the password set on the PFX certificate earlier.
- Select *Manual PEM* as the type for CA Trusted Roots and upload the “root.cer” file. (*Note:* When updating this certificate, the CA Certificate also needs to be re-uploaded)
- Test both certificates by clicking on “show certificate”. If both are OK and don’t give any errors you can continue.
- Verify that the Username Claim URL points to the UPN property of the SAML response. Single Sign-On can only work when using the UPN.
- Click Apply

Show Certificate

To validate if your certificate is correct you can visualize the certificate's content using the *Show Certificate* button.

End User Flow:

The end user flow will be similar to the one from Pre-Authentication except that the step where the user needs to enter their Windows Password again will no longer appear:

- When a user accesses the Awingu landing page, Awingu will check if the user has a valid authentication token with the configured IDP.
- If this is not the case yet Awingu will redirect the browser to the IDP. User will need to authenticate first against the IDP. If successful, the IDP will redirect the User to the Awingu landing page.
- User will be logged into the Awingu Workspace
- From the Workspace they can start Apps, Desktops and get access to the Drives.

From a technical point of view once a user has pre-authenticated, Awingu will now use the UPN that was received from the IdP to create an X.509 client certificate suitable for smart-card login. These client certificates are valid for 1 day. Using the client certificate, Awingu request a Kerberos Ticket Granting Ticket (TGT) from the Active Directory Domain Controller through PKINIT. To complete the login to Awingu, Awingu fetches the attributes and group memberships of the user from the Active Directory Domain Controller. These attributes are required for other functionality in Awingu to work, for example, to decide if a user has admin rights or if the user is allowed access to certain drives, applications or features of Awingu.

In order to setup an RDP session using Awingu, we must perform two authentication steps, the network level authentication (NLA) and Windows logon:

- The NLA is done using the same Kerberos TGT acquired earlier. We currently support up to CredSSP version 6 for this authentication step.
- For the Windows logon, Awingu emulates a smart card designed to work with the Windows standard drivers. This virtual smart card appears to contain the X.509 client certificate that was generated earlier.

Note: When SSO is configured, the Change Password link in the Account Settings of the users will not be visible to avoid confusion about which password will be changed (IdP or AD).

Microsoft OneDrive for Business

Introduction

Users of OneDrive for Business can have their home drive shown on the Files page in Awingu. They can do all actions as with normal drives, like upload, download, copy, move, rename, delete, preview, except of opening a file with a streamed application.

We describe in this section how to configure both your Microsoft account and your Awingu environment.

Allowing Awingu to access your Office 365 subscription

In order to allow your Awingu environment to access the OneDrive of your Office 365 subscription, Microsoft provides following documentation:

> https://dev.onedrive.com/app-registration.htm#register-your-app-for-onedrive-for-business

That document is however somewhat outdated, so we summarize here the steps to take.

Step 1. Get an Office 365 subscription

All Office 365 subscriptions for Small Businesses and Enterprises should be compatible with Awingu. Even the smallest package, Office 365 Business Essentials, works fine.

The procedure dictates to get an Office 365 Developer Site:

1. Go to https://portal.office.com > Admin
2. Resources > Sites
3. Click on "Add a site"
4. Fill in all the fields like you desire
   For following fields, please note:
    - Template Selection: Developer Site
    - Server Resources: default value should be enough

   Click OK and you end-up in the SharePoint admin center (direct link: https://<your_account>-admin.sharepoint.com)
5. The new developer site URL in the Site Collections list.
6. When the site creation is finished (spinning wheel next to the URL), you can navigate to the URL to open your Developer Site.
   This takes a long time (up to one hour).

Step 2. Set up an Azure Active Directory tenant

Make sure your Office 365 subscription is synced with Azure AD.

Step 3. Register your app with Azure Active Directory

1. Go to https://portal.azure.com
2. Open the service: App registrations
3. Click on New registration:
    a. Name: e.g. "OneDrive on Awingu"
    b. Supported account types: Accounts in any organizational directory (Any Azure AD directory - Multitenant)
    c. Redirect URI:
        i. Web
        ii. URL: the URL to your Awingu environment (e.g. https://awingu.mycompany.com)
4. Once created, retrieve the Client ID = Application ID.
   You will need this value to configure Awingu.
5. Click on Certificates & secrets and click New client secret
    a. Description: secret
    b. Expires: Never
    c. Click on Save

    d. Retrieve Client secret = secret
       You will need this value to configure Awingu.
       ⚠ The value cannot be retrieved afterwards. Don't loose it!

6. Click on API permissions and click on Add a permission:
    a. Select an API: Office 365 SharePoint Online
    b. Select permissions: Read and write user files (delegated permission)
    c. Click on Done

Step 4. Have the network right

Awingu needs to be able to reach the OneDrive for Business servers directly, or through an HTTP proxy (see Connectivity Settings). HTTPS (port 443) access is required to:

- <mydmain>**-my**.sharepoint.com
- graph.microsoft.com
- api.office.com

Configuring Awingu to access OneDrive

OneDrive for Business can be configured as Drive in the System Settings. Go to Manage > Drives and add a drive with following settings:

- Name: e.g. OneDrive
- Description
- Backend: ONEDRIVE
- Client ID: see previous section
- Client secret: see previous section
- Workspace URL: the URL a user uses to access Awingu, e.g. https://awingu.mycompany.com
- Redirect URL: you will need this value to configure Azure Active Directory
- URL: link to your sharepoint.com environment, e.g. https://mycompany.sharepoint.com
- UNC: can be left empty
- Labels: you can use labels to group drives together. You can leave this empty.
- User Labels: the drive will only be visible for users with a matching user label. Use "all:" to assign the drive to all users.

Configuring the Awingu OneDrive app

1. Go to https://portal.azure.com
2. Go to Azure Active Directory > App registrations
3. For your app (e.g. OneDrive on Awingu), go to Manage > Authentication
4. Under Web > Redirect URIs > add the Redirect URL you've obtained in System Settings
5. Press Save

Using OneDrive on Awingu

When a user opens their OneDrive folder on the Files page in Awingu for the first time, they will be redirected to the Office login portal where access is requested to their OneDrive. Once access is granted, they can use OneDrive as any other folder in Awingu, except of opening a file with a streamed application (only open with Preview will work).

Smart Card Redirection

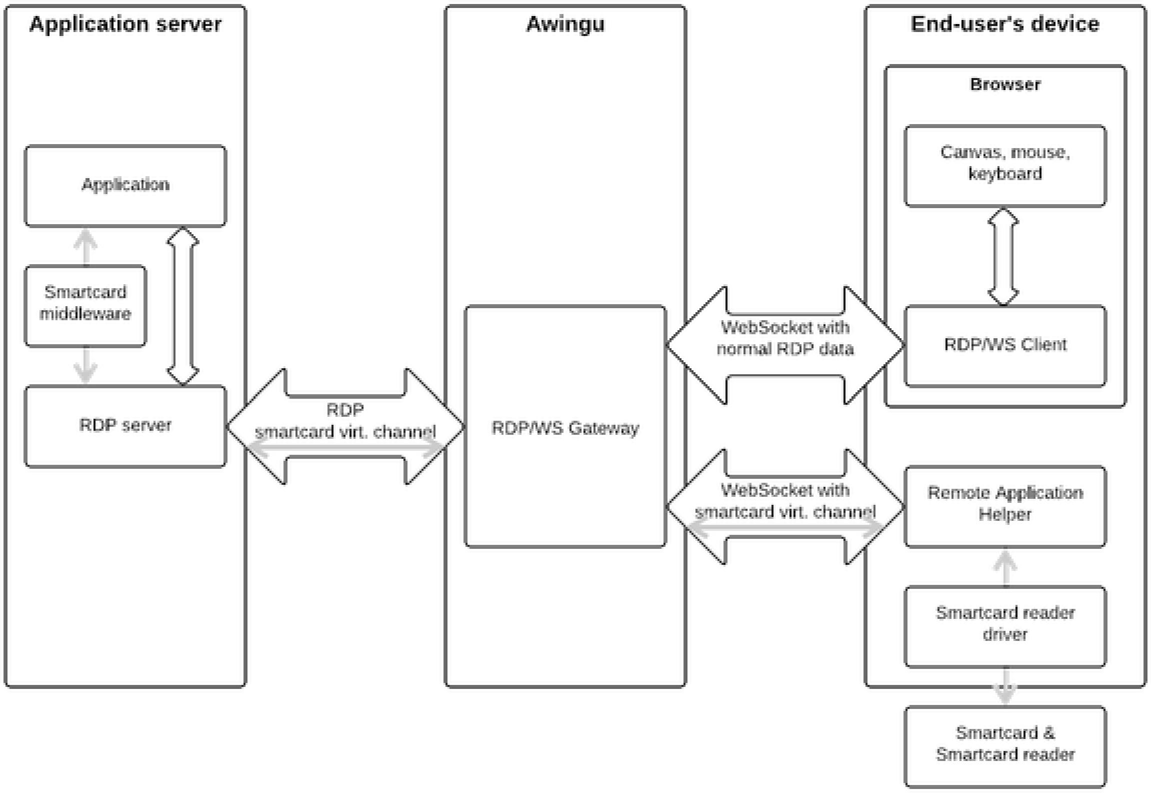
Introduction

Awingu supports accessing smart cards in streamed applications. This enables a user to access a smart card connected to his client device (e.g. a smart card reader in his laptop) from an application running on an application server. Typical use cases include electronic ID cards, banking cards or access cards. This does not include using smart cards as second factor authentication for accessing the Awingu portal.

Although any smart card should work, Awingu has explicitly tested the following smart cards:

- Belgian eID
- Dutch UZI pas
- Italian InfoCert Business Key
- Isabel

How It Works



In order to use a smart card in a streamed application, the administrator should explicitly enable smart card support for the application and the user should dispose of a smart card reader connected to his device. When the user launches such a smart card support enabled application, the Awingu portal will connect to the locally installed Remote Application Helper, which will connect to the smart card reader and act as a bridge between the smart card reader and the Awingu portal.

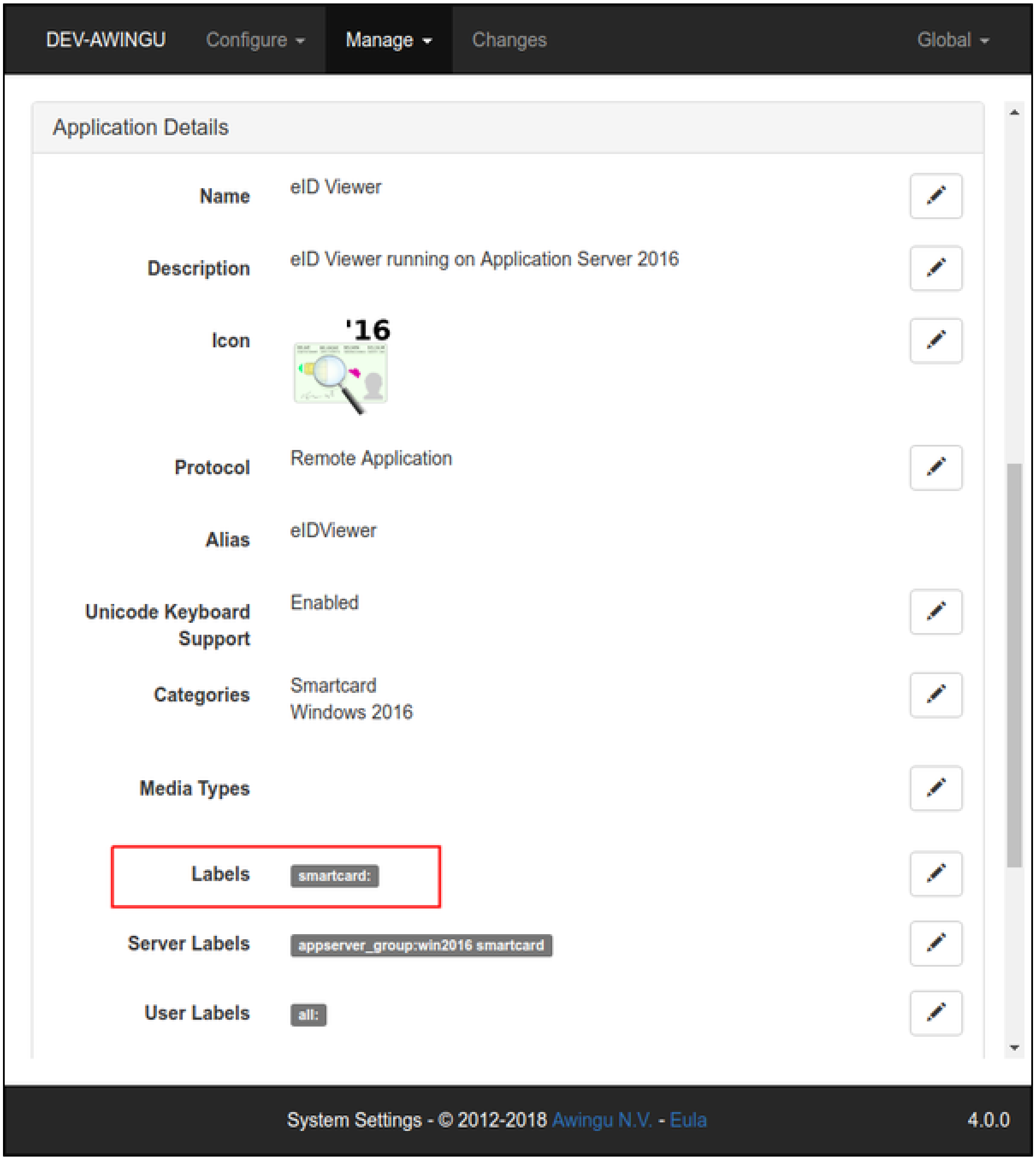
Enabling smart card support

Preparing the application server

The application server should have the middleware installed of the smart card.

Enabling smart card access on Awingu

To enable smart card access to an RDP or RemoteApp application, the *smartcard:* label should be assigned to the application. This can be set in the details of an application in the *System Settings* under *Manage > Applications*



Application Details

Name	eID Viewer
Description	eID Viewer running on Application Server 2016
Icon	'16
Protocol	Remote Application
Alias	eIDViewer
Unicode Keyboard Support	Enabled
Categories	Smartcard Windows 2016
Media Types	
Labels	smartcard:
Server Labels	appserver_group:win2016 smartcard
User Labels	all:

Once this label is assigned to an application, the application will try to connect to the Remote Application Helper.

Enabling smart card access on the client

The first time a user launches a smart card enabled application, the browser will ask the user to download the Remote Application Helper. This software can be downloaded from the Awingu appliance and is available for Windows and macOS.

Note that for macOS, the installer is not signed: the user needs to do right-click > Open on the installer.

The user needs to have the drivers of the smart card reader installed on their device. Note that some drivers are included in the operating system and don't need any end-user intervention.

Limitations

1. Smart card functionalities don't work anymore once the application session has been disconnected (e.g. opened in another browser window). In this case, the application has to be opened again.
2. The smart card reader needs to be connected before opening the application.

3. The libraries to communicate with smart cards differ slightly between Windows and macOS. Therefore, it might be that some applications on the Windows application server will perform certain library call that is incompatible with the macOS library available on the end-user device. We have seen this behavior for the eID Viewer and Isabel.
4. The Remote Application Helper will use a proxy on the client if it detects a configured proxy on Windows. The Remote Application Helper cannot be configured to use a proxy on MacOS.

Troubleshooting

- Check whether the driver of the smart card reader is installed on the user's device;
- Check whether the middleware of the smart card is installed on the application server.
- When Firefox has been installed after the installation of the Remote Application Helper, the Remote Application Helper needs to be re-installed.
- When the user did not stop Firefox during the installation (as requested in the installer), the Remote Application Helper needs to be re-installed.
- When using clients with Windows 7 Embedded, you will need to install Visual C++ 2015 redistributable (32-bit/x86 version) on them. It is a known issue that you need to install KB2999226 first to be able to install Visual C++ 2015.

Automate Awingu via the REST API

Awingu provides a REST API allowing to install, configure and manage Awingu. This allows you to integrated Awingu in an automation framework.

Getting Started with the Awingu API

This section assumes:

- You have an installed Awingu appliance running.
- You have a domain configured.
- You have the correct tools to execute REST API calls (e.g. PowerShell, see below).

To test it out manually, you can use as tool to execute the REST API calls

- The live API browser at http(s)://your-awingu-environment/api/v2/
- The API documentation at http(s)://your-awingu-environment/api/v2/docs/

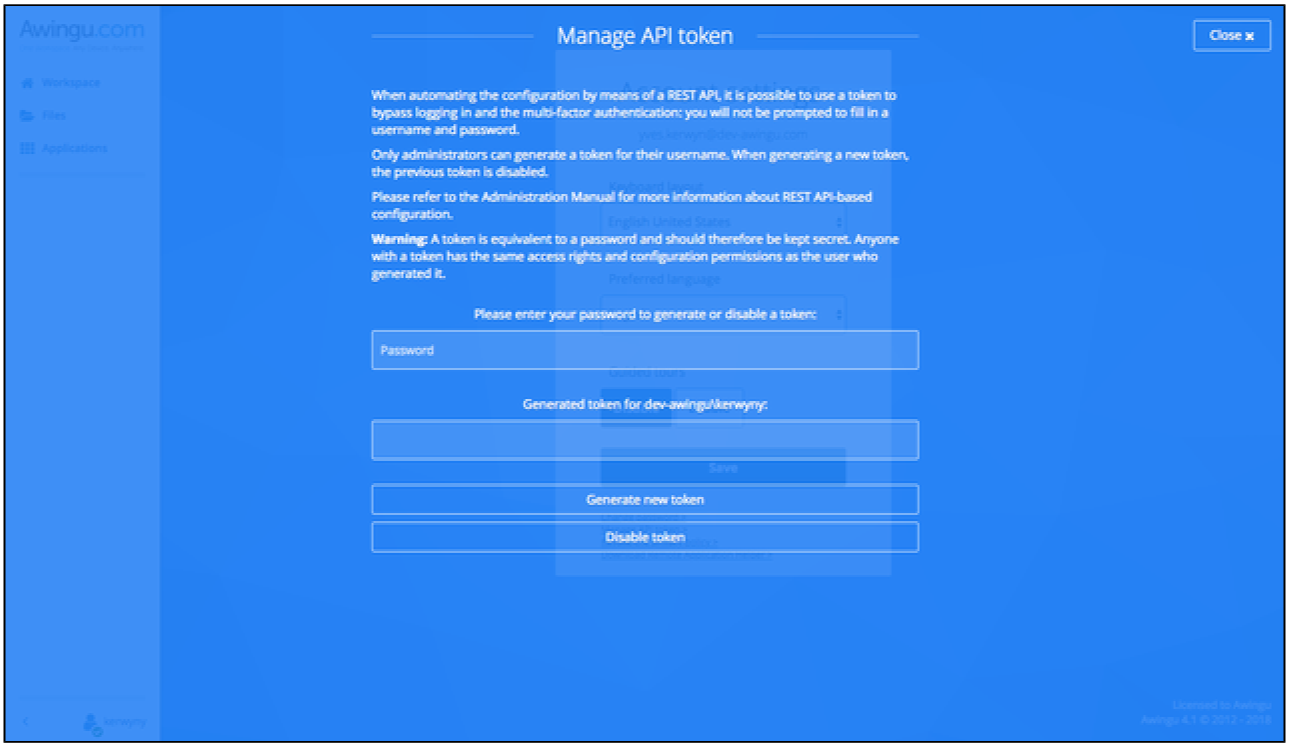
Note: all API call are addressed to port 80 of the appliance.

PowerShell example using an API Token

If enabled for the domain, admin users with can get an API token to interact with the REST API.

See User Connector Configuration for information on how to limit API token based authentication to certain subnets.

In order to get an API token go to your **Account settings** and click **Manage API token**, which will bring a dialog window for generating a token.



Manage API token

When automating the configuration by means of a REST API, it is possible to use a token to bypass logging in and the multi-factor authentication: you will not be prompted to fill in a username and password.

Only administrators can generate a token for their username. When generating a new token, the previous token is disabled.

Please refer to the Administration Manual for more information about REST API-based configuration.

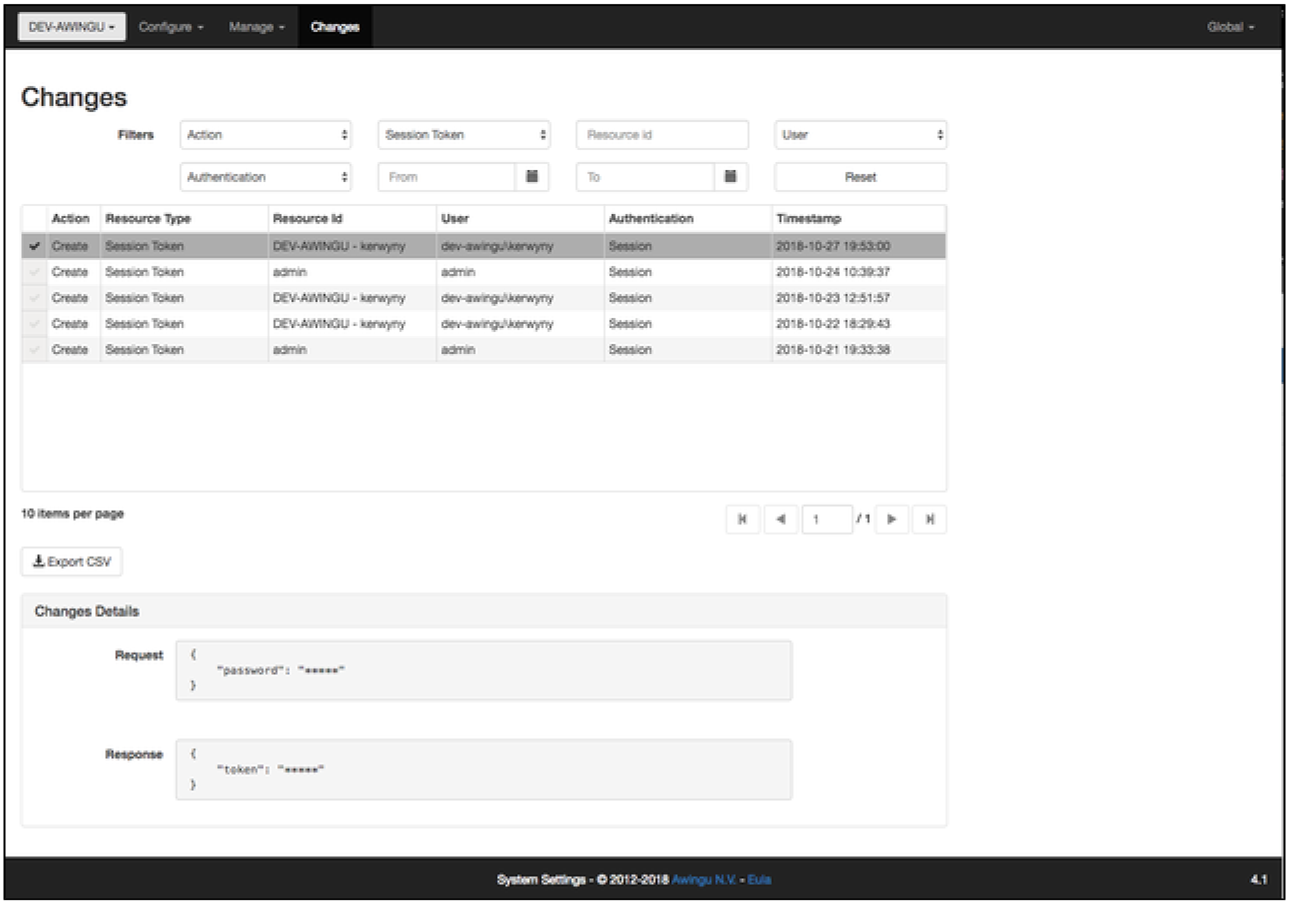
Warning: A token is equivalent to a password and should therefore be kept secret. Anyone with a token has the same access rights and configuration permissions as the user who generated it.

Please enter your password to generate or disable a token:

Generated token for dev-awingu\kerwyny:

Note that API tokens continue to be valid even when the user was removed from Active Directory, or when removed from the admin group.

For an audit trace of the API tokens check **Changes** for your domain in **System Settings**, and filter on **Session Token** as **Resource Type**.



Changes

Filters: Action | Session Token | Resource id | User | Authentication | From | To

	Action	Resource Type	Resource Id	User	Authentication	Timestamp
✓	Create	Session Token	DEV-AWINGU - kerwyny	dev-awingu\kerwyny	Session	2018-10-27 19:53:00
	Create	Session Token	admin	admin	Session	2018-10-24 10:39:37
	Create	Session Token	DEV-AWINGU - kerwyny	dev-awingu\kerwyny	Session	2018-10-23 12:51:57
	Create	Session Token	DEV-AWINGU - kerwyny	dev-awingu\kerwyny	Session	2018-10-22 18:29:43
	Create	Session Token	admin	admin	Session	2018-10-21 19:33:38

10 items per page

1 / 1

Changes Details

Request

```
{
    "password": "*****"
}
```

Response

```
{
    "token": "*****"
}
```

With the API token you can consume the REST API from PowerShell as shown in the below example, listing all application servers:

```
$token = "<your API token here>"
$your_uri = "https://<address of your appliance here>/api/v2/app-servers
/"

[Net.ServicePointManager]::SecurityProtocol = [Net.
SecurityProtocolType]::Tls13

$headers = @{}
$headers.Add("Authorization", "Token $token")

$result = Invoke-RestMethod -Method get -Uri $your_uri -Headers $headers
$result.results | Format-Table
```

Navigating Through the API

- To list the URIs to all available system resources:

```
URI:     /api/v2/
Method:  GET
Headers: Accept: */*
         Authorization: Token your-api-token
```

Expected response: 200 with following payload:

```
{
    "branding": "http://172.16.5.74/api/v2/branding/",
    "branding-images": "http://172.16.5.74/api/v2/branding-images/",
    "favicons": "http://172.16.5.74/api/v2/favicons/",
    "domains": "http://172.16.5.74/api/v2/domains/",
    "hostheaders": "http://172.16.5.74/api/v2/hostheaders/",
    "certificates": "http://172.16.5.74/api/v2/certificates/",
    "apps": "http://172.16.5.74/api/v2/apps/",
    "app-servers": "http://172.16.5.74/api/v2/app-servers/",
    "app-icons": "http://172.16.5.74/api/v2/app-icons/",
    "user-apps": "http://172.16.5.74/api/v2/user-apps/",
    "key-combos": "http://172.16.5.74/api/v2/key-combos/",
    "configuration": "http://172.16.5.74/api/v2/configuration/",
    (...)
}
```

- To retrieve an system resource, e.g. the drives, you can use the URI mentioned in the output of the previous command:

```
URI:     /api/v2/drives/
Method:  GET
Headers: Accept: */*
         Authorization: Token your-api-token
```

Expected response: 200 with following payload:

```
{
    "count": 31,
    "next": null,
    "previous": null,
    "results": [
        {
            "backend": "CIFS",
            "config": [],
            "description": "Home Drive via CIFS",
            "domain": "http://172.16.5.74/api/v2/domains/2/",
            "name": "Home Drive",
            "unc": "\\\\fileserver\\Users$\\<username>\\Documents",
            "url": "smb://fileserver.mycompany.com/Users$/<username>
/Documents",
            "use_domain": false,
            "labels": [],
            "user_labels": [
                "all:"
            ],
            "uri": "http://172.16.5.74/api/v2/drives/1/",
            "smb_max_protocol": "SMB3"
        },
        (...)
    ]
}
```

For more information about this resource, you can use your web browser to navigate to http(s)://your-awingu/api/v2/docs/#drives

Changing Settings

- To add a resource, e.g. to add a drive to a domain:

```
URI:     /api/v2/drives/
Method:  POST
Headers: Content-Type: application/json
         Accept: */*
         Authorization: Token your-api-token
         Referer: http://your-awingu-env/
Payload: {
             "domain": "http://172.16.5.74/api/v2/domains/2/",
             "name": "New Drive",
             "description": "This is a drive to test the API",
             "backend":"CIFS",
             "config": [],
             "url": "smb://fileserver.mycompany.com/TestShare",
             "unc": "\\\\fileserver\\TestShare",
             "use_domain": false,
             "labels": ["testkey:testlabel"],
             "user_labels": ["all:"]
         }
```

  Expected response: 201, with the URI of the drive in the payload.
  Note that the API will automatically create the labels and user_labels provided in case they don't exist. You can verify this in `/api/v2/labels/`

- To change fields of an existing resource, e.g. change the unc field of a drive:

```
URI:     /api/v2/drives/9/
Method:  PATCH
Headers: Content-Type: application/json
         Accept: */*
         Authorization: Token your-api-token
         Referer: http://your-awingu-env/
Payload: {"unc": "\\\\fileserver\\Share"}
```

Logging Out

```
URI:     /api/v2/sessions/current/
Method:  DELETE
Headers: Accept: */*
```

```
         Content-Type: application/json
         Authorization: Token your-api-token
         Referer: http://your-awingu-env/
```

Expected response: 204

Further documentation

All available API resources are documented on your appliance on /api/v2/docs/.

Installing with the Awingu API

1. Deploy the Awingu appliance and configure the networking, which can be automated with the API tools provided by the virtualization or cloud platforms in combination with DHCP.
2. Once the VM has been started, the installer API will start to listen on **port 8080**.
3. To start the installation, do following call on port 8080. Please refer to Awingu Installer for more information about the fields used in the request.

```
URI:     /api/v2/updates/install/
Method:  POST
Headers: Accept: */*
         Content-Type: application/json

Payload: {
           "config": {
             "eula": {
               "accepted": true
             },
             "network": {
               "dns": "172.19.0.1",
               "ntp": "ad.mycompany.com"
             },
             "environment": {
               "management_user": {
                 "username": "my-admin-user",
                 "password": "my-password",
                 "confirmed_password": "my-password"
               }
             },
             "appliances": [
               {
                 "ip_address": "172.19.0.2",
                 "hostname": "awingu"
               }
             ],
             "features": {
               "common": {
                 "external_database": false
               }
             }
           }
         }
```

Expected response: 201 with payload:

```
{
  "uri": "http://172.16.5.76:8080/api/v2/updates/1/",
  "progress": [],
  "begin": "2017-10-20T11:04:24",
  "end": null,
  "status": "IN_PROGRESS",
  "service": null,
  "version": "http://172.16.5.76:8080/api/v2/versions/1/",
  "outputs": "http://172.16.5.76:8080/api/v2/update-outputs/?update=1"
}
```

4. Wait until the installer has finished:

```
URI:     /api/v2/updates/1/
Method:  GET
Headers: Accept: */*
```

If field "status" can be IN_PROGRESS, SUCCEEDED or FAILED.
The error output can be retrieved via the outputs field of the response:

```
URI:     /api/v2/update-outputs/?update=1
Method:  GET
Headers: Accept: */*
```

Configuring with the Awingu API

Once the installation is done, you can configure Awingu as follows:

1. Enable an API token for the management user configured during the installation.
2. Add your first domain via POST to /api/v2/domains/.
   Hostheaders are autogenerated if you provide a list of FQDNs in the "hostheaders" field.
   The user connector is configured in the same domain resource.
3. User groups, like for admin, are added via /api/v2/user-groups/
4. Application servers are added via /api/v2/app-servers/
   For each application server, a server label is automatically created and linked to it.
5. Icons for applications are uploaded via /api/v2/app-icons/create/
6. Applications are added via /api/v2/apps/, where you need to provide the link to the uploaded app-icon.
   Provided labels (labels, user_labels, server_labels), categories and media-types are automatically created if they don't exist yet.
7. Drives are added via /api/v2/drives.
   Provided labels (labels, user_labels) are automatically created if they don't exist yet.

Please refer to the documentation on /api/v2/docs/ to have more information of the payload to provide.

External Audit Logging

Introduction

Awingu allows you to forward all audit logs to an external system using the HTTP(S) protocol.

Each record will be transmitted to the configured URL using an `HTTP POST` per record in `JSON` format.

Structure

A record is a collection of unordered key/value pairs (an `Object` in `JSON` terms) providing information of the audit event for the specific `audit_type`.

All records provide the following properties:

Property	Type	Description
`audit_type`	String	The audit record type
`version`	String	Awingu version

Based on the `audit_type` you can discriminate between audit record types and interpreter the specific properties of each type.

The `version` field represents the Awingu version and allows you to version your integrations.

Audit Records Types

User Sessions

User Session records represent a single authenticated session between a browser and the Awingu environment for a user. If a user logs in for a second time on a different browser, this will result in a new session.

User sessions are also the basis for licensing, e.g. the number of concurrent users is determined based on the number of simultaneous active sessions.

Property	Type	Description
`audit_type`	String	Record type (`usersessions`)
`version`	String	Awingu version
`session_id`	String	Unique id
`session_start`	DateTime	Timestamp when the session started in UTC
`session_end`	DateTime	Timestamp when the session ended in UTC
`session_labels`	String	A comma-separated list of all labels assigned to the user for this session
`username`	String	Username
`domain`	String	Name of the Awingu domain
`ip`	String	The IP address of the client that created this session
`http_agent`	String	Value of the `User-Agent` header when creating this session

`country`	String	Country from where the session was created based on GeoIP
`geoip_latitude`	String	Latitude from where the session was created based on GeoIP
`geoip_longitude`	String	Longitude from where the session was created based on GeoIP
`name`	String	Browser name based on `User-Agent`
`major`	String	Browser version major based on `User-Agent`
`minor`	String	Browser version minor based on `User-Agent`
`os`	String	Client operating system based on `User-Agent`
`os_name`	String	Client operating system name based on `User-Agent`

Application Sessions

Application Sessions represent a single streamed application or desktop session for a user. Every time a new streamed application or desktop connection is started, a new application session is generated.

ℹ Web applications and reverse proxied web applications are logged separately as Web Application Sessions

Property	Type	Description
`audit_type`	String	Record type (`appsessions`)
`version`	String	Awingu version
`userapp_session_id`	UUID	Unique id
`user_session_id`	String	Reference to the *User Session* that started the *Application Session*
`ip`	String	The IP address of the client starting the application
`appsession_start`	DateTime	Timestamp when the application session started in UTC
`appsession_end`	DateTime	Timestamp when the application session ended in UTC
`app_key`	UUID	Identifier of the application started
`domain`	String	Name of the Awingu domain the application is configured
`server`	String	Host name of the application server the application is started on
`port`	String	The port op the application server used to start the application
`exe`	String	The alias of the RemoteApp (empty for RDP applications)
`recorded`	Boolean	Indicated if the *Application Session* is recorded or not
`rdpgw_session_id`	UUID	The internal id for the connection between the browser and Awingu
`rdpgw_numeric_id`	String	The internal id for the connection between the browser and Awingu

Web Application Sessions

Web Application Sessions represent web applications launched from the Awingu portal or access to a reverse proxied web application using the configured source host header or launched from the Awingu portal.

Property	Type	Description
`audit_type`	String	Record type (`webappsessions`)
`version`	String	Awingu version
`user_session_id`	String	Reference to the *User Session* that started the *Web Application Session*
`timestamp`	DateTime	Timestamp when the *Web Application Session* started in UTC

`url`	Sting	URL used to access the web application
`name`	String	Name of the web application configured
`domain`	String	Name of the Awingu domain the web application is configured
`reverse_proxy`	Boolean	Indicated if the web application started is a reversed proxied web application

Application Gateway

The Application Gateway is an internal component that determines a.o. on which application server an application can be started and also keeps track of the status of all application sessions. It manages both *Application Sessions* and *Web Application Sessions*.

The audit records of this component allow you to track changes in the state of all application sessions.

Property	Type	Description
`audit_type`	String	Record type (`appgw`)
`version`	String	Awingu version
`timestamp`	DateTime	The timestamp of the status change
`username`	String	Username of the user owning the application session
`session_id`	UUID	Reference to the *User Session* that started the *Web Application Session*
`session_labels`	String	A comma-separated list of all labels assigned to the user for the referenced *User Session*
`domain`	String	Name of the Awingu domain the application is configured
`appname`	String	Name of the application
`appkey`	UUID	Identifier of the application
`labels`	String	A comma-separated list of all labels assigned to the application
`user_labels`	String	A comma-separated list of all user labels assigned to the application
`server_labels`		A comma-separated list of all server labels assigned to the application
`appsession_id`	UUID	*Application Session* id
`status`	String	New status of the application session
`host`	String	Host name of the application server the application is started on
`gateway_id`	String	Name of the Awingu appliance handling the application session
`document`	String	UNC path to the document opened with the application

File Actions

A *File Action* represents a file operation executed through the Awingu portal, this does not include file operations executed by streamed applications.

Property	Type	Description
`audit_type`	String	Record type (`file_actions`)
`version`	String	Awingu version
`timestamp`	DateTime	The timestamp of the action
`session_id`	UUID	Reference to the *User Session* that executed the file action
`action`	String	Action executed on the file
`domain`	String	Name of the Awingu domain the drive is configured

`drive`	String	Name of the drive the file action was executed on
`destination_drive`	String	Name of the destination drive if the file action results on another drive
`file_path`	String	The relative path of the file on the drive
`destination_file_path`	String	The relative path of the file on the destination drive if the file action results on another drive

Shares

Property	Type	Description
`audit_type`	String	Record type (`shares`)
`version`	String	Awingu version
`timestamp`	DateTime	The timestamp of the action
`session_id`	UUID	Reference to the *User Session* that executed the file action
`action`	String	Action executed on the share
`domain`	String	Name of the Awingu domain the share is configured
`share_id`	UUID	Unique ID of the share
`share_name`	String	Name of the share
`share_content_type`	String	Content-type of the share
`share_expires`	DateTime	The expiry date of the share
`share_drive`	String	Name of the drive the share is part of
`share_domain`	String	Name of the Awingu domain the share is configured
`share_created_by`	String	Username of the user that created the share
`share_path`	String	The relative path of the file on the drive
`share_mode`	String	Availability mode of the share
`share_is_public`	String	Is the share publicly available
`share_access_rights`	String	How are the access rights determined?
`share_access_labels`	String	Which users/groups can access the share when `share_access_rights` is USER
`share_checksum`	String	The checksum of the shared file (when accessed)
`share_has_password`	String	Is the share password protected
`ip`	String	The IP address of the client performing the action
`country`	String	The country based on GeoIP of the client accessing the share
`geoip_latitude`	String	The latitude based on GeoIP of the client accessing the share
`geoip_longitude`	String	The longitude based on GeoIP of the client accessing the share
`range`	String	Range accessed during request

Shared Application Session

A *Shared Application Session* represents a guest that joined or leaves a shared application session.

Property	Type	Description
`audit_type`	String	Record type (`sharedappsessions`)

`version`	String	Awingu version
`userapp_session_id`	UUID	Reference to the *Application Session* that is shared
`sharedappsession_start`	DateTime	The timestamp on which the client joined the shared application session
`sharedappsession_end`	DateTime	The timestamp on which the client left the shared application session
`rdpgw_session_id`	String	The internal id for the connection between the browser (guest) and Awingu
`rdpgw_numeric_id`	String	The internal id for the connection between the browser (host) and Awingu
`ip`	String	The IP address of the client that joined the shared application session
`domain`	String	Name of the Awingu domain the application session is part of

Shared Application Session Settings

A *Shared Application Session Setting* represents a change in the configuration of a shared application session.

Property	Type	Description
`audit_type`	String	Record type (`sharedappsessions_settings`)
`version`	String	Awingu version
`timestamp`	DateTime	The timestamp of the action
`user_session_id`	String	Reference to the *User Session* that started the *Application Session*
`userapp_session_id`	UUID	Reference to the *Application Session* that is shared
`rdpgw_session_id`	UUID	The internal id for the connection between the browser (guest) and Awingu
`joinable`	Boolean	Is the application session shared
`isProtected`	Boolean	Is the shared application session password protected
`joinMode`	String	always `SINGLE`
`accessRights`	String	Is the session shared in `PUBLIC` or `DOMAIN` mode
`host`	String	The hostname of the Awingu appliance handling the application session
`domain`	String	Name of the Awingu domain the application session is part of

IdP Sessions

IdP Sessions represent Awingu acting as IdP for web applications and confirming a user’s identity based on the Awingu session.

Property	Type	Description
`audit_type`	String	Record type (`idpsessions`)
`version`	String	Awingu version
`login_time`	DateTime	The timestamp an external SSO Service requests Awingu to identify a user
`logout_time`	DateTime	The timestamp the *Users Session* ended
`user_session_id`	String	Reference to the *User Session* for which the SSO Service requests was made
`username`	String	The username for which the SSO Service requests was made
`service_provider_name`	String	Name of the service provider, as mentioned in User Connector Configuration

`domain`	String	Name of the Awingu domain the *User Session* is part of
`assertion_consumer_service`	String	ACS URL, as configured for the SSO service
`request_issuer`	String	The issuer, as configured for the SSO service
`request_id`	String	SAML request ID, provided by the SSO service

Anomalies

An anomaly represents an unusual activity detected by the Awingu environment. More information on the type of anomalies can be found in Anomaly Reporting.

Property	Type	Description
`audit_type`	String	Record type (`anomalies`)
`version`	String	Awingu version
`timestamp`	DateTime	The timestamp of the event
`session_id`	String	Reference to the *User Session* if the user is logged in
`code`	String	Anomaly code
`category`	String	Anomaly category
`description`	String	Anomaly description
`username`	String	The username used for the login
`domain`	String	Name of the Awingu domain the *User Session* is part of
`http_agent`	String	The `User-Agent` header of the client
`ip`	String	The IP address of the client
`country`	String	The country based on GeoIP of the client
`geoip_latitude`	String	The latitude based on GeoIP of the client
`geoip_longitude`	String	The longitude based on GeoIP of the client
`fingerprint`	String	The generated fingerprint of the client (`NEW_BROWSER`)
`attempts`	String	The number of failed login attempts (`TOO_MANY_FAILED_ATTEMPTS`)
`distance_km`	String	Distance in km (`TRAVEL_SPEED`)
`distance_mi`	String	Distance in mi (`TRAVEL_SPEED`)
`speed_kmh`	String	Speed in km/h (`TRAVEL_SPEED`)
`speed_mph`	String	Speed in mi/h (`TRAVEL_SPEED`)
`existing_countries`	String	A comma-separated list of countries for existing *User Sessions* for the user (`COUNTRY_MISMATCH`)

Backup and recovery of the Awingu Database

Introduction

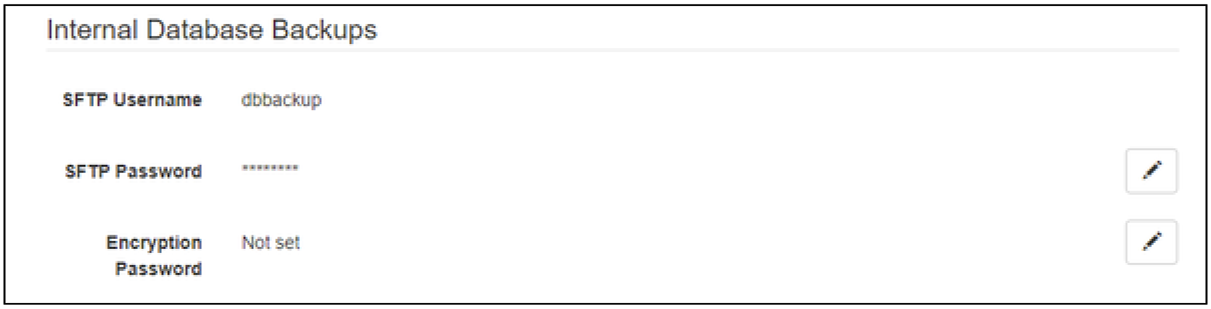
The Awingu platform allows to generate an off-site backup of the internal database.

This section does not apply when using an external database. To backup an external database, please refer to the snapshot capabilities of MS SQL or PostgreSQL.

Backup

Awingu saves the database to local disk every day. You can retrieve this database dump and save it on another system via SFTP so that in case of a database or disk failure, you can recover your Awingu environment.

System Settings > Global > Connectivity > Internal Database Backups



Internal Database Backups

SFTP Username dbbackup

SFTP Password ********

Encryption Password Not set

- **SFTP Username:** The read-only SFTP username is set to *dbbackup*
- **SFTP Password:** The password of the SFTP user. Change this password to be able to connect to retrieve the database dumps.
- **Encryption Password:** Password to use to encrypt the database backups. Backups will not be encrypted when no password is set. Encrypted backups have the '.enc' extension and will require this password to be able to restore the backup.

The dump of the database is done every night at midnight. The dumps are retained on local disk for a period of 3 days, before being discarded.

To download the database dump from the Awingu environment:

- you need an SFTP capable client (graphical tool: filezilla; Linux command-line: sftp)
- Connect to the IP or FQDN of the datastore node, on port 22. For a single node VM, the datastore is located on the Awingu VM.
- Enter the username/password defined in System Settings
- You will find the recent database backups in the folder postgres.

Restore

To recover from a broken database, you can upload a previously downloaded dump to the Awingu appliance via SFTP or use a dump which is still available on the Awingu appliance.
You can list the available dumps on an appliance by executing the database-list-backups action from the Troubleshoot page.

Same configuration and credentials apply for downloading or uploading dumps using SFTP.

After you uploaded a dump to restore to, you can execute the database-restore-backup action from the Troubleshoot page.

If you restored to fresh new appliance, you will need to re-enter the Certificate and Private key (per domain: Configure > User Connector > Federated Authentication) when Single Sign-On is configured.

Some data are not stored into the database and won't be recovered:

- Insights (in the Dashboard) (prior to 5.1 and when migrate audit logs was not completed yet)
- Audit (in the Dashboard) (prior to 5.1 and when migrate audit logs was not completed yet)
- Metering data (in the Dashboard)

⚠ Restoring a database is only supported to an appliance with the same hostname and of the same Awingu version.