

Awingu.com

One Workspace. Any Device. Anywhere.

Awingu Admin Guide

Version 4.1

1. Awingu Admin Guide 4.1 Home	3
1.1 Document Guidance	4
1.2 Installation	5
1.2.1 Connectivity Requirements	6
1.2.2 Sizing Requirements	8
1.2.3 Deployment	10
1.2.3.1 Deployment on Microsoft Hyper-V	11
1.2.3.2 Deployment on VMware ESXi with vSphere Client on Windows	19
1.2.3.3 Deployment on VMware ESXi with vSphere Web Client	31
1.2.3.4 Deployment on Linux KVM	38
1.2.3.5 Deployment on Microsoft Azure	46
1.2.3.6 Deployment on Amazon EC2	47
1.2.3.7 Deployment on Google Compute	48
1.2.4 Awingu Installer	49
1.2.5 Azure Awingu All-In-One	55
1.3 System Settings	60
1.3.1 System Settings - Global	61
1.3.1.1 Connectivity Settings	62
1.3.1.2 General Information	66
1.3.1.3 Service Management Settings	70
1.3.1.4 Domain Settings	72
1.3.1.5 Certificate Settings	75
1.3.1.6 Troubleshoot	78
1.3.2 System Settings - Configure	82
1.3.2.1 Branding Configuration	83
1.3.2.2 Feature Configuration	86
1.3.2.3 User Connector Configuration	88
1.3.3 System Settings - Manage	96
1.3.3.1 Application Management	97
1.3.3.2 Application Server Management	104
1.3.3.3 Category Management	107
1.3.3.4 Drive Management	108
1.3.3.5 File Type Management	111
1.3.3.6 Label Management	113
1.3.3.7 User Management	118
1.3.4 System Settings - Change Log	119
1.3.5 Service Provider Support in Awingu	121
1.4 How it works	129
1.4.1 Sign-in Process	130
1.4.2 Streamed Applications	132
1.4.3 Reversed Proxied Web Applications	134
1.5 Monitoring and Reporting	140
1.5.1 Status Overview of Services on All Servers	141
1.5.2 Monitoring Servers and Components	142
1.5.3 Awingu License Tracking	143
1.5.4 Live Monitoring of Users Activity	144
1.5.5 Monitoring the Application Connector	145
1.5.6 Insights Reporting	146
1.5.7 Audit Reporting	147
1.5.8 Anomaly Reporting	151
1.6 Integration	153
1.6.1 Integrating with existing Windows environment	154
1.6.2 Using Awingu on existing Citrix infrastructure	162
1.6.3 SSL offloader, reverse proxy or loadbalancer settings	168
1.6.4 Multi Factor Authentication	173
1.6.4.1 Using Awingu built-in OTP	174
1.6.4.2 Integrating Awingu with Azure MFA	175
1.6.4.3 Integrating Awingu with DUO	176
1.6.5 Single Sign-On for SaaS Applications	180
1.6.5.1 Single Sign-On for Azure AD - Office 365	181
1.6.5.2 Single Sign-On for Google Apps	187
1.6.5.3 Single Sign-On for Okta	193
1.6.5.4 Single Sign-On for Salesforce	197
1.6.6 Microsoft OneDrive for Business	201
1.6.7 Microsoft Skype for Business Online	203
1.6.8 Smart Card Redirection	205
1.6.9 Automate Awingu via the REST API	208
1.7 Backup and recovery of the Awingu Database	215

Awingu.com

One Workspace. Any Device. Anywhere.

Awingu

Admin Guide

Version 4.1

- [Document Guidance](#)
- [Installation](#)
- [System Settings](#)
- [How it works](#)
- [Monitoring and Reporting](#)
- [Integration](#)
- [Backup and recovery of the Awingu Database](#)

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	<i>Awingu User Guide 4.1</i>
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
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 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): <ul style="list-style-type: none">• UDP port 137, TCP port 445 (direct TCP enabled)• UDP port 137 broadcast, TCP port 139 (direct TCP disabled)	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	<ul style="list-style-type: none"> • 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): <ul style="list-style-type: none"> • Microsoft OneDrive for Business: <ul style="list-style-type: none"> • <mydomain>-my.sharepoint.com • login.microsoftonline.com • graph.microsoft.com • Microsoft Skype for Business Online: <ul style="list-style-type: none"> • *.online.lync.com • *.infra.lync.com • login.microsoftonline.com • DUO Multi-Factor Authentication: <ul style="list-style-type: none"> • <your_api>.duosecurity.com • Automatic certificates through Let's Encrypt (see Certificate Settings): <ul style="list-style-type: none"> • *.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***	<ul style="list-style-type: none"> • 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***	<ul style="list-style-type: none"> • 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)

* 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).

Awingu only works well when the end-user accesses Awingu via port 80 or 443. When using NAT, port 80 (HTTP) or port 443 (HTTPS) should be used towards the customer (meaning that browsing to <http://awingu.mycompany.com:81> won't work well).

Sizing Requirements

Awingu Sizing Requirements

Single node Awingu

In a single node set-up, all processes are running on a single VM. This architecture can support only a limited number of the concurrent sessions. This is not a hard limit, but a limit that has been determined during in-depth performance testing cycles. For these tests, Awingu has used average user profiles (3 streamed applications, 10 accesses to reverse proxied web applications, a number of file operations per hour per user). This has resulted in the following deployment recommendations:

Number of Concurrent Users	20	50	75	100
Memory (GiB)	4	4	6	8
vCPUs	2	4	6	8

Note however 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. An Awingu environment has exactly 1 or 3 backends (whether or not high availability is required) and 1 or more frontends.

Multi node without high availability

If high availability is not required, i.e. service interruption is allowed until the broken appliance has been restored from snapshot or re-installed, then you can scale-up to 100 users with a single node. Up to 200 users, you can still use the internal database. When using more than 200 users, you will need to use an external database (cf. [Installation](#)). Note that you cannot change from an internal to an external database!

Number of concurrent users	Appliances with backend and frontend	Appliances with only frontend	External DB
Max. 150	1 x (8 GiB / 8 vCPUs)	1 x (4 GiB / 4 vCPUs)	Optional
Max. 200	1 x (8 GiB / 8 vCPUs)	1 x (4 GiB / 8 vCPUs)	Optional
Max. 300	1 x (8 GiB / 8 vCPUs)	2 x (4 GiB / 8 vCPUs)	Required
Max. 400	1 x (8 GiB / 8 vCPUs)	3 x (4 GiB / 8 vCPUs)	Required

For each extra 100 users, add a frontend-only appliance of 4 GiB / 8 vCPUs.

If the CPU load on the first node is getting to high (thousands of users), you can move away the frontend role from that node.

Multi node with high availability

If high availability is required, i.e. service interruption is not allowed (except during upgrades), then you need a multi node and an external database (cf. [Installation](#)) from the beginning. Note that if an appliance goes down, the users that have their RDP connections opened towards the applications servers via that appliance, will lose their connection and unsaved changes. They will however connect to another appliance for next RDP connection.

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

Backup strategy

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.

Soft HA

One appliance might fall out without noticeable performance degradation for the users.

Number of concurrent users	Appliances with backend and frontend	Appliances with only frontend	External DB
Max. 50	3 x (6 GiB / 2 vCPUs)	none	Required
Max. 100	3 x (6 GiB / 4 vCPUs)	none	Required
Max. 200	3 x (8 GiB / 8 vCPUs)	none	Required
Max. 300	3 x (8 GiB / 8 vCPUs)	1 x (4 GiB / 8 vCPUs)	Required
Max. 400	3 x (8 GiB / 8 vCPUs)	2 x (4 GiB / 8 vCPUs)	Required

For each extra 100 users, add a frontend-only appliance of 4 GiB / 8 vCPUs.

If the CPU load on the first three nodes is getting to high (thousands of users), you can move away the frontend role from those nodes.

Hard HA

One rack (out of three) might fall out without noticeable performance degradation for the users. The 3 backend nodes are in different racks and the frontend nodes are evenly spread over the racks.

Number of concurrent users	Appliances with backend and frontend	Appliances with only frontend	External DB
Max. 50	3 x (6 GiB / 2 vCPUs)	none	Required
Max. 100	3 x (6 GiB / 4 vCPUs)	none	Required
Max. 200	3 x (8 GiB / 8 vCPUs)	none	Required
Max. 400	3 x (8 GiB / 8 vCPUs)	3 x (4 GiB / 8 vCPUs)	Required
Max. 600	3 x (8 GiB / 8 vCPUs)	6 x (4 GiB / 8 vCPUs)	Required

For each extra 200 users, add three frontend-only appliances of 4 GiB / 8 vCPUs.

If the CPU load on the first three nodes is getting to high (thousands of users), you can move away the frontend role from those nodes.

Application Server Sizing Requirements

As a rule of thumb, Awingu recommends one physical Windows application server per 100 concurrent users, with a minimum of 2 for redundancy. If virtualized, then 4 Windows application server virtual machines per physical machine, with each 4 cores, 32 GB RAM serving up to 25 concurrent users.

Deployment

For your convenience, Awingu provides virtual appliances that are custom-built to run on three commonly used hypervisors, i.e. VMware ESXi, Microsoft Hyper-V and Linux KVM, 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.

- [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

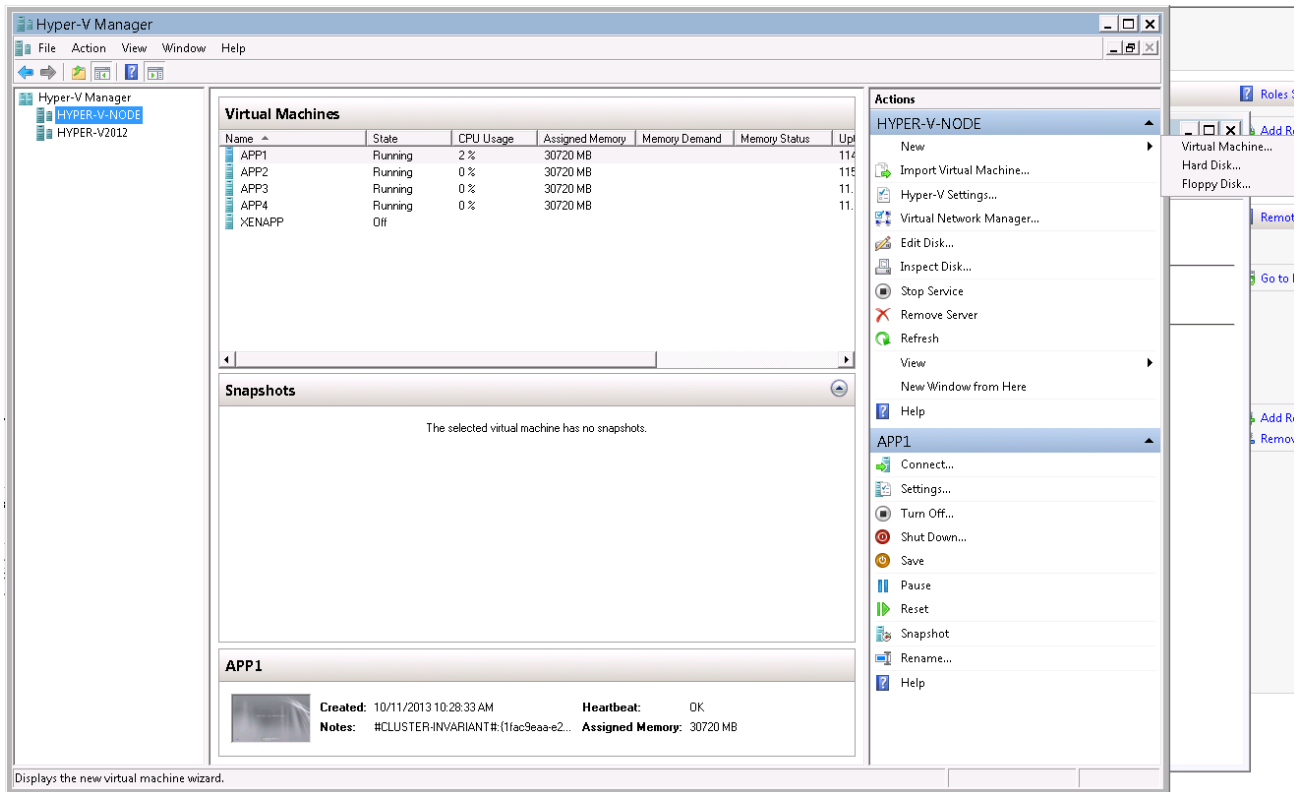
- Step 1 - Download and extract the Awingu appliance
- Step 2 - Create a VM with the VHD image in Hyper-V manager
- Step 3 - Start up the Awingu virtual machine

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".



2. Specify a name for the Awingu virtual machine

New Virtual Machine Wizard

Specify Name and Location

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

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:

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

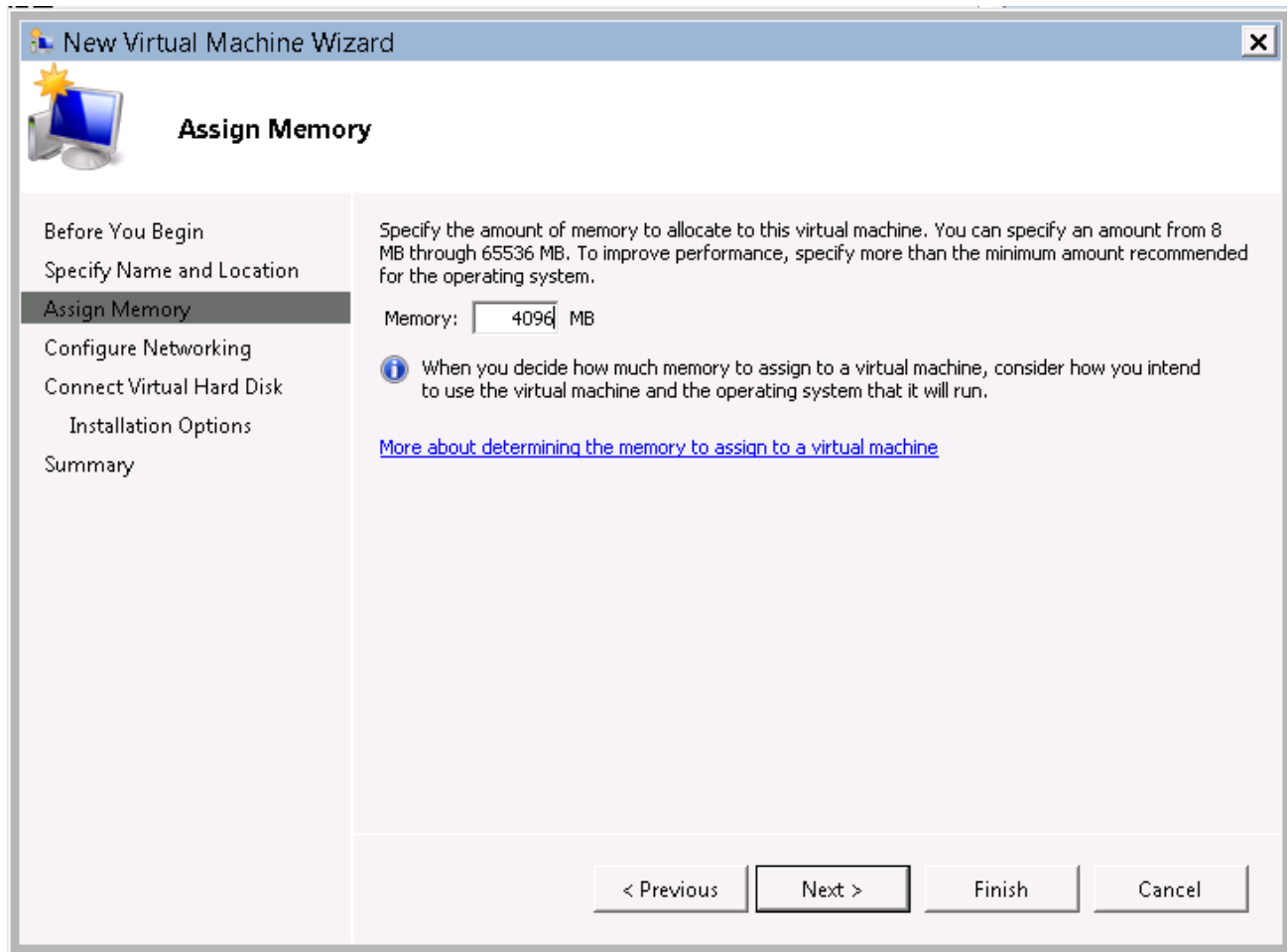
Location:

 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.

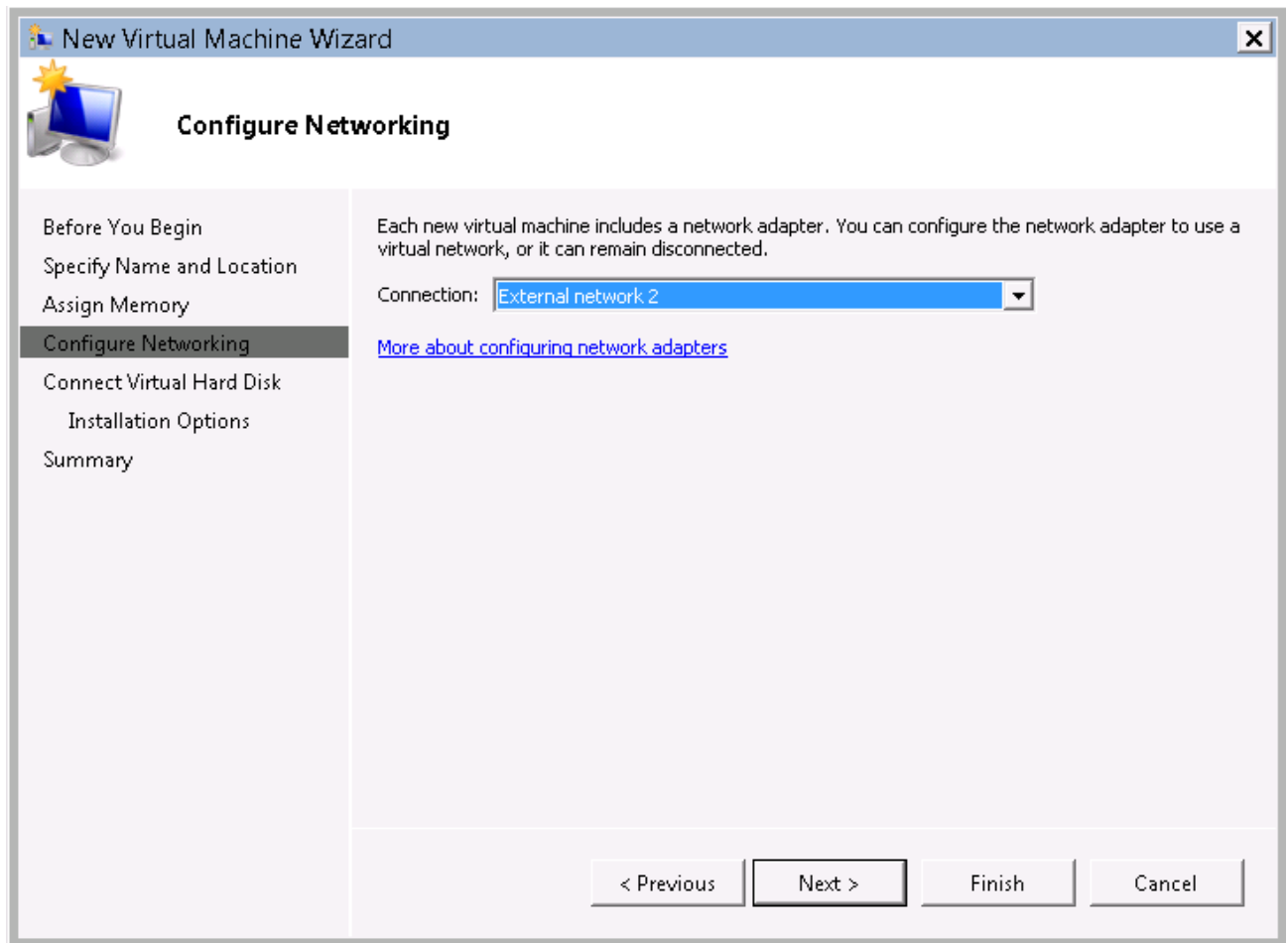
< Previous Next > Finish Cancel

3. Assign memory to the Awingu virtual machine:
4. Specify RAM and CPU settings for your VM:

Number users	RAM
20 concurrent users	4096 MiB
50 concurrent users	4096 MiB
100 concurrent users	8192 MiB



5. Configure networking for your Awingu virtual machine



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

New Virtual Machine Wizard

Connect Virtual Hard Disk

Before You Begin
Specify Name and Location
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary

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:

Location:

Size: GB (Maximum: 2040 GB)

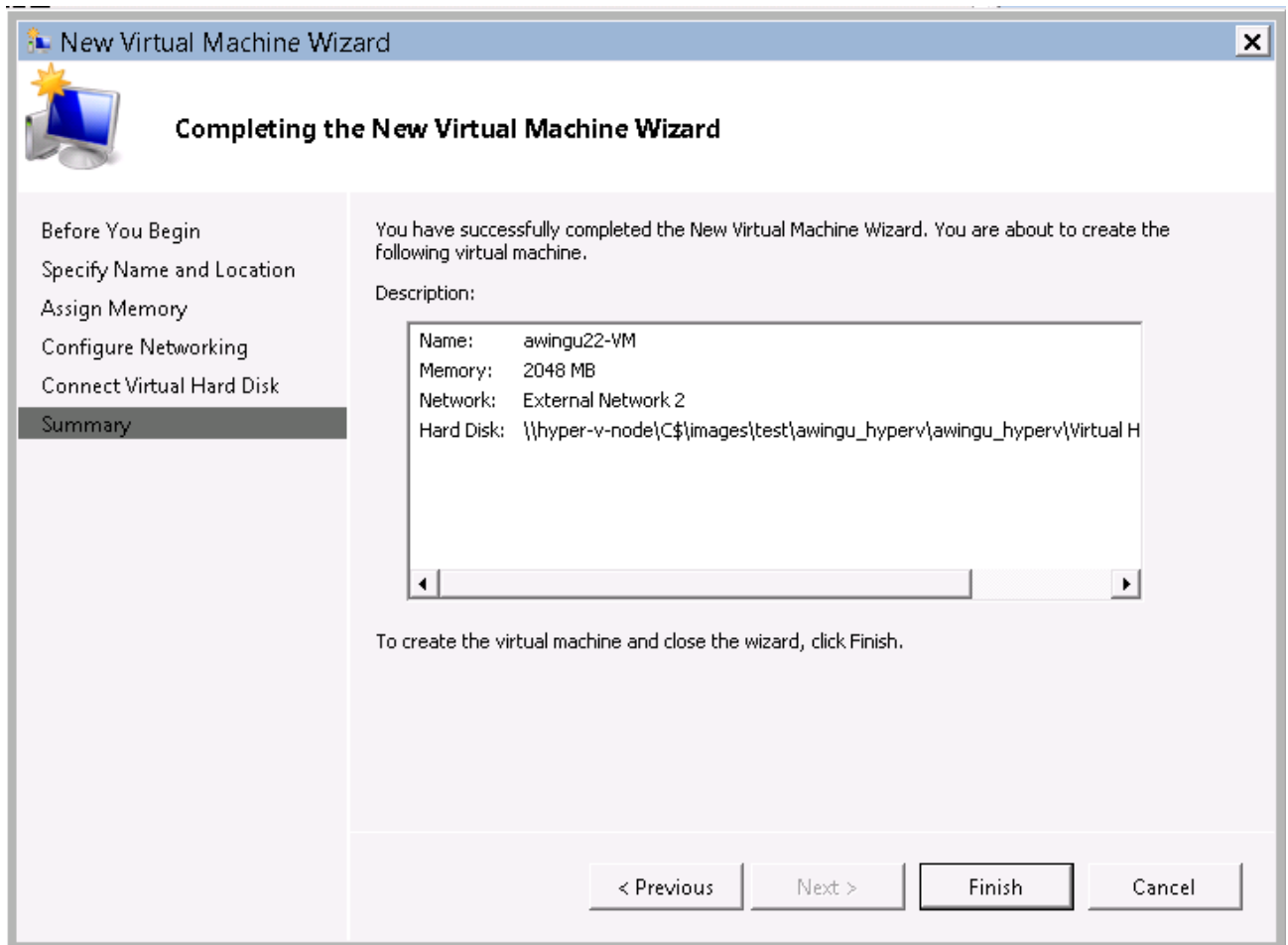
☒ Use an existing virtual hard disk

Location:

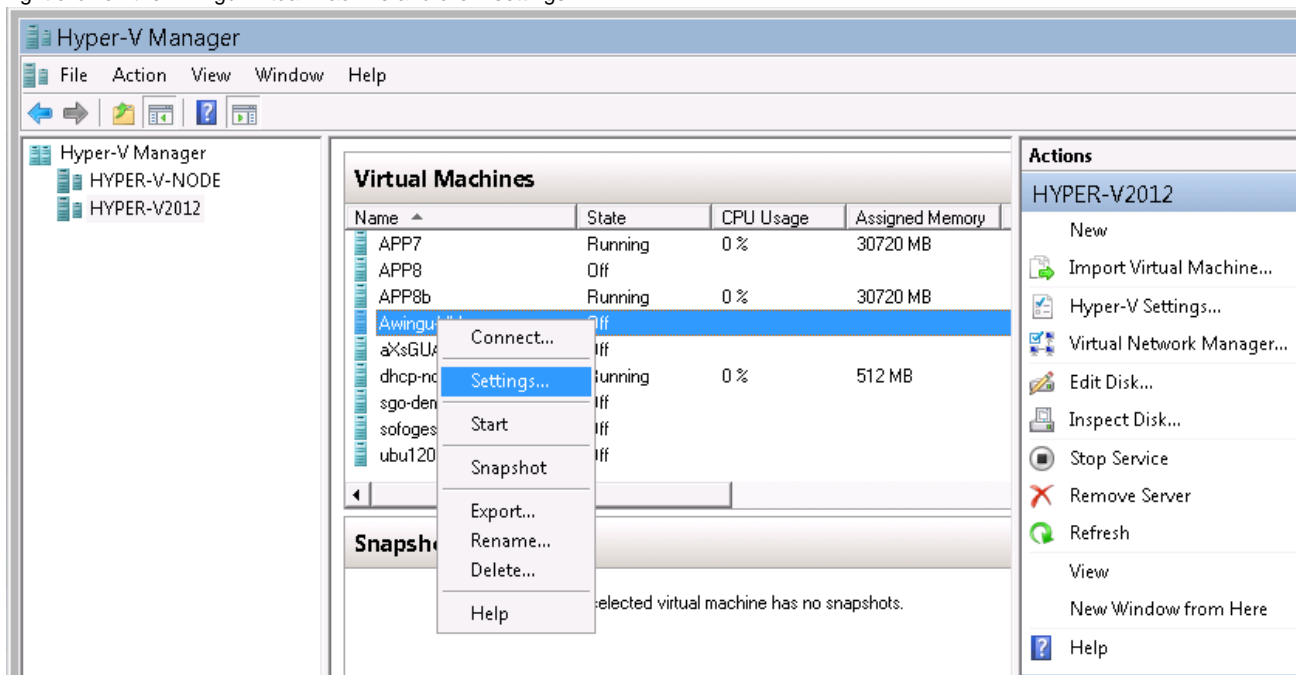
☐ Attach a virtual hard disk later

< Previous Next > Finish Cancel

7. Review your virtual machine settings

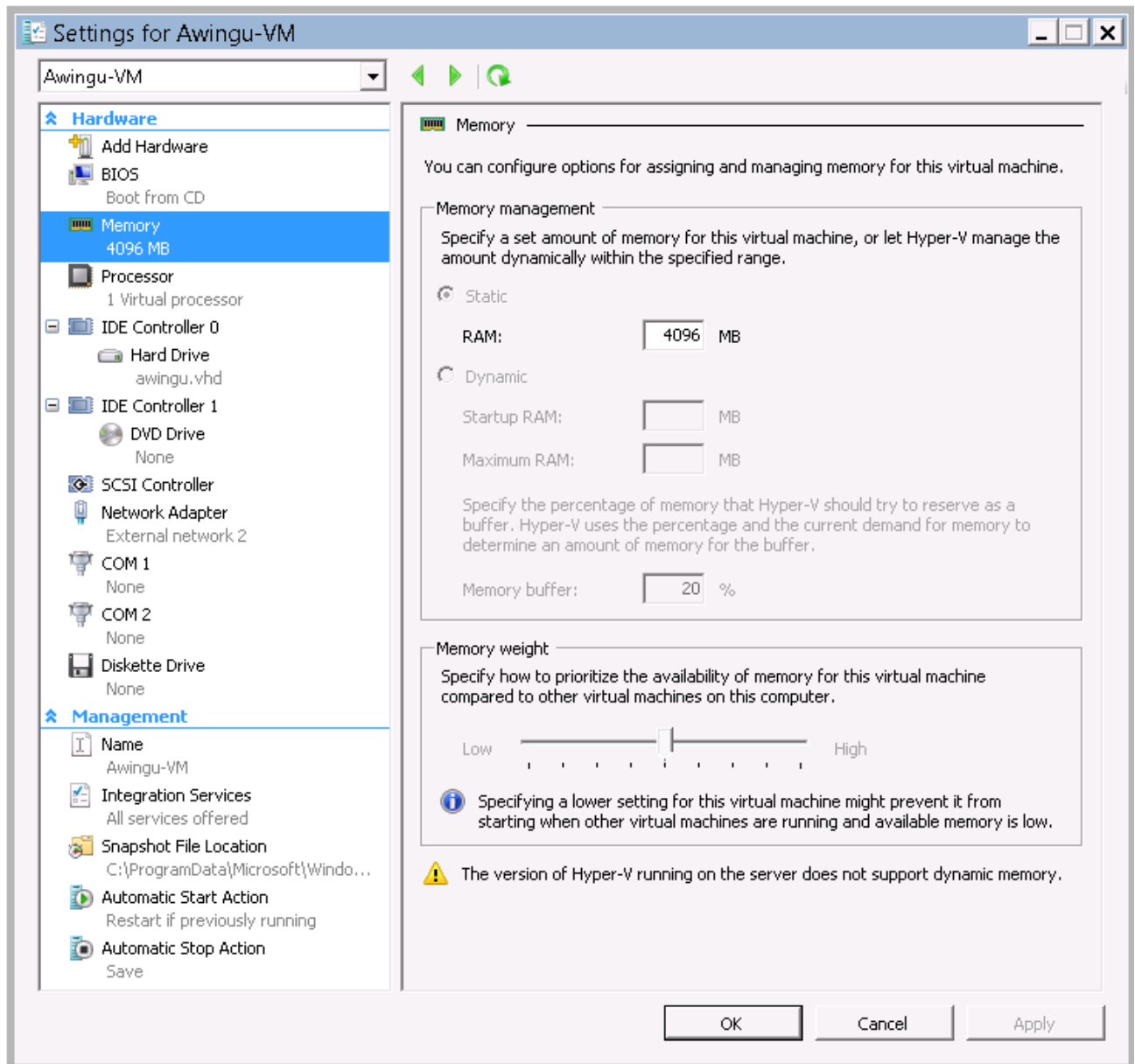


8. Right click on the Awingu Virtual machine and click "settings..."



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.

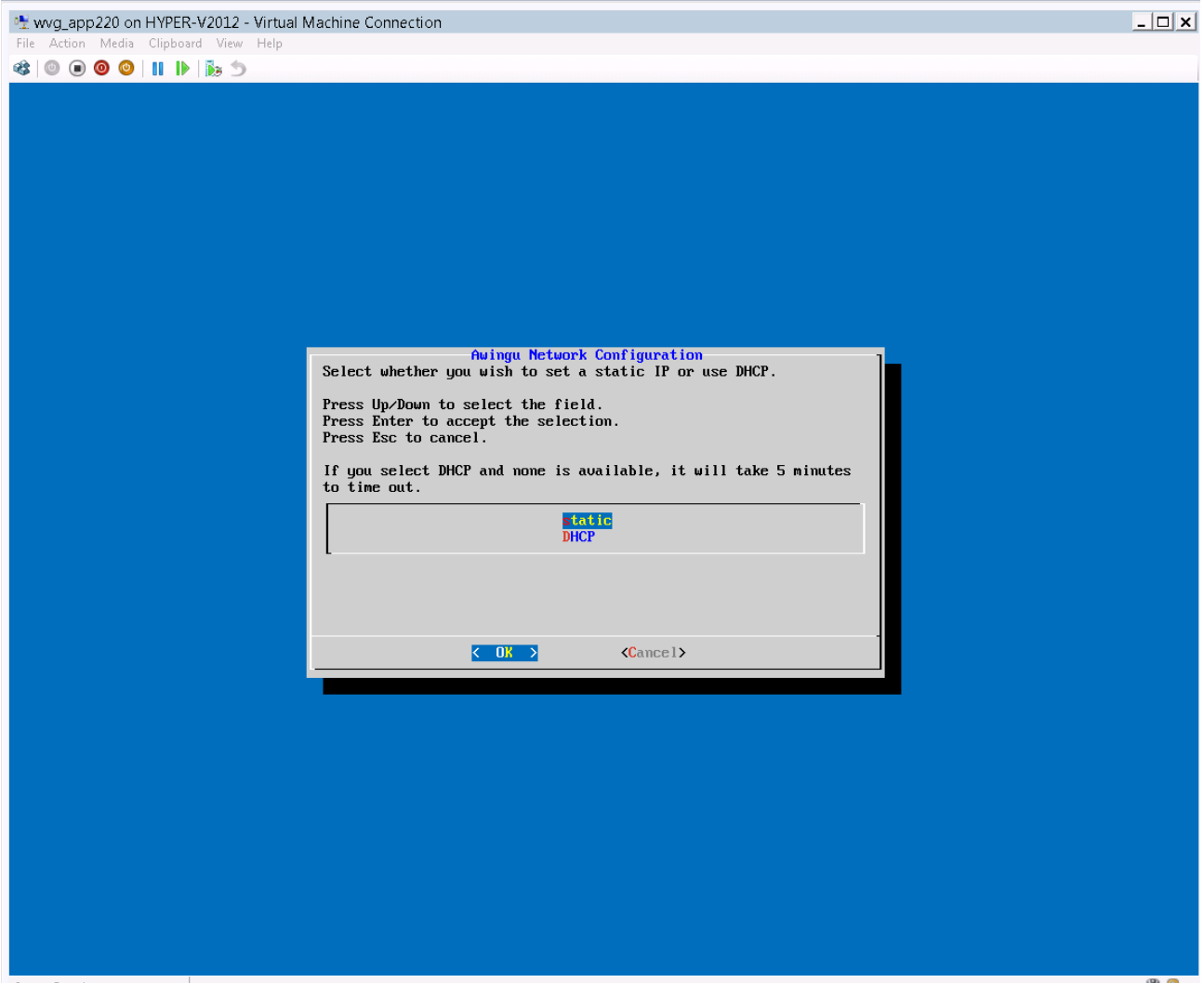


Awingu recommends the following specs for your virtual machine. Those specs are based on carefully performed internal load tests.

Number users	CPUs
20 concurrent users	2 CPUs
50 concurrent users	4 CPUs
100 concurrent users	8 CPUs

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.



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](#).

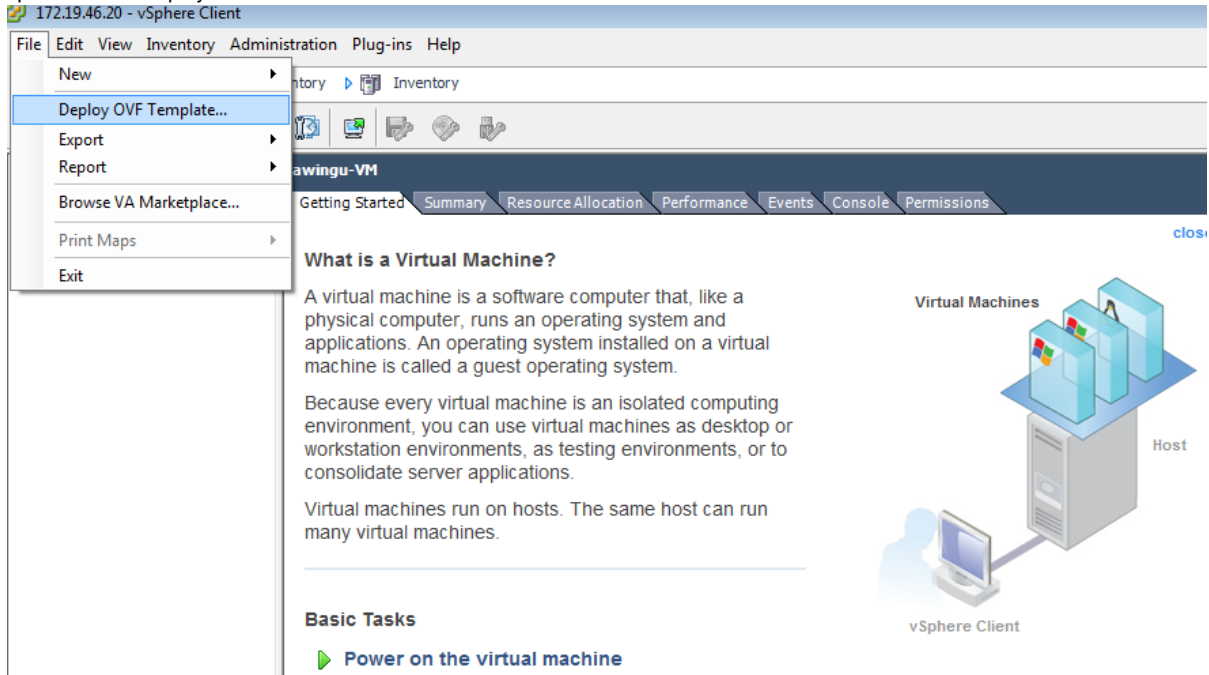
Deployment on VMware ESXi with vSphere Client on Windows

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

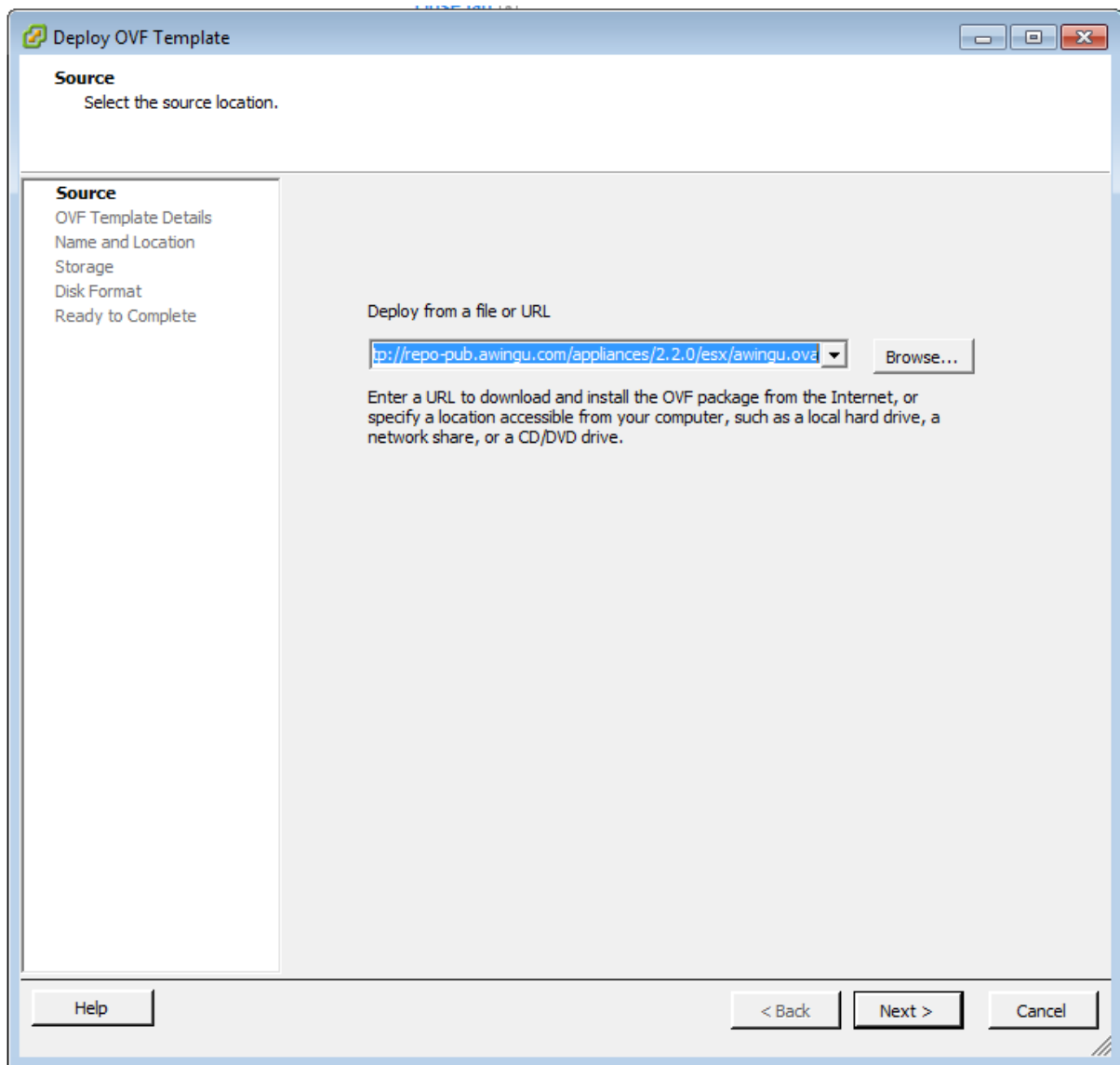
- Step 1 - Import the appliance in VMware vSphere Client
- Step 2 - Configure your Awingu virtual machine settings
- Step 3 - Start up your Awingu virtual machine

Step 1 - Import the appliance in VMware vSphere Client

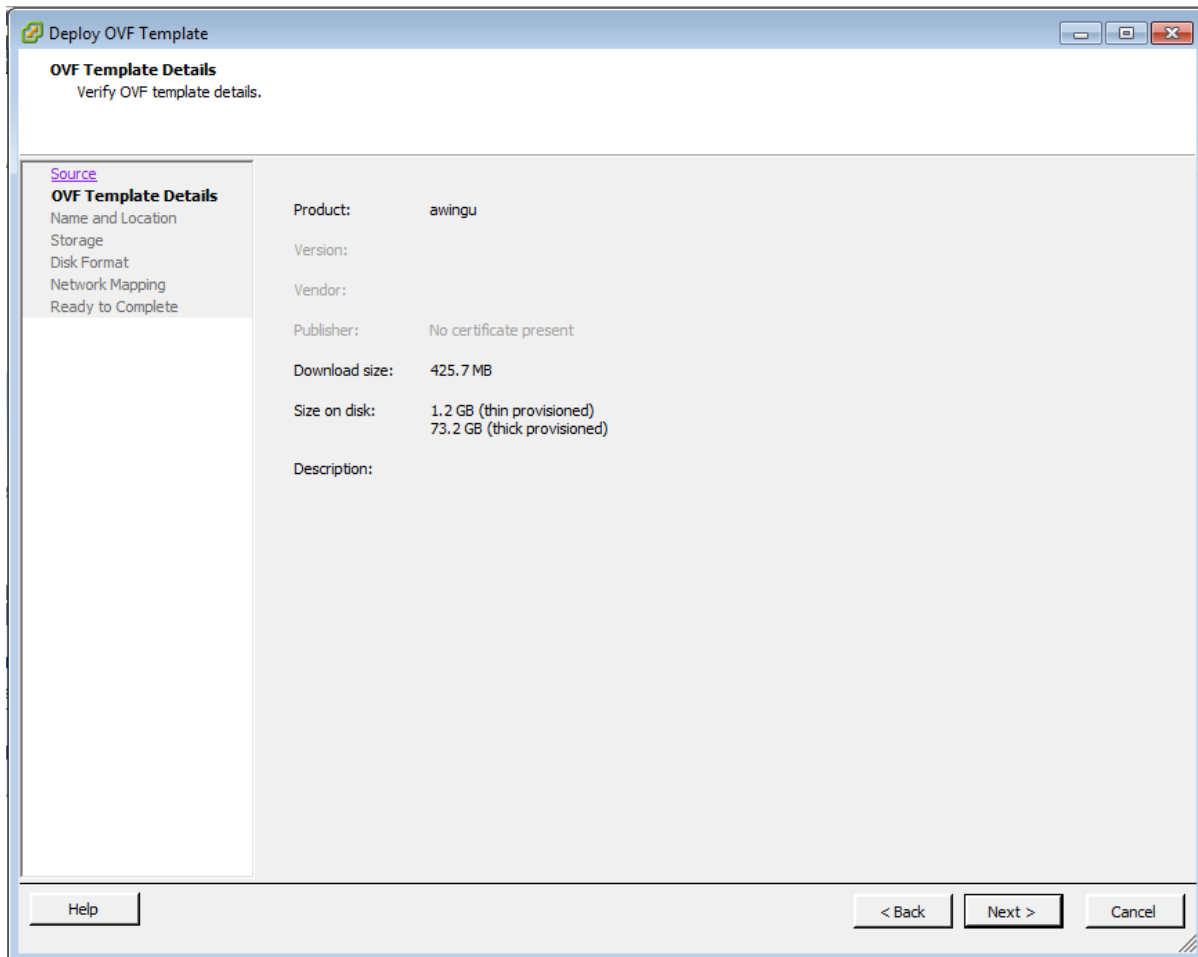
1. Connect to your vSphere ESXi hypervisor using vSphere Client
2. Open the OVF deployment menu



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>



- c. Alternatively, you can download the OVA file and use it via the Browse... button.
- 4. Verify the template details



5. Enter the name for your Awingu virtual machine

Deploy OVF Template

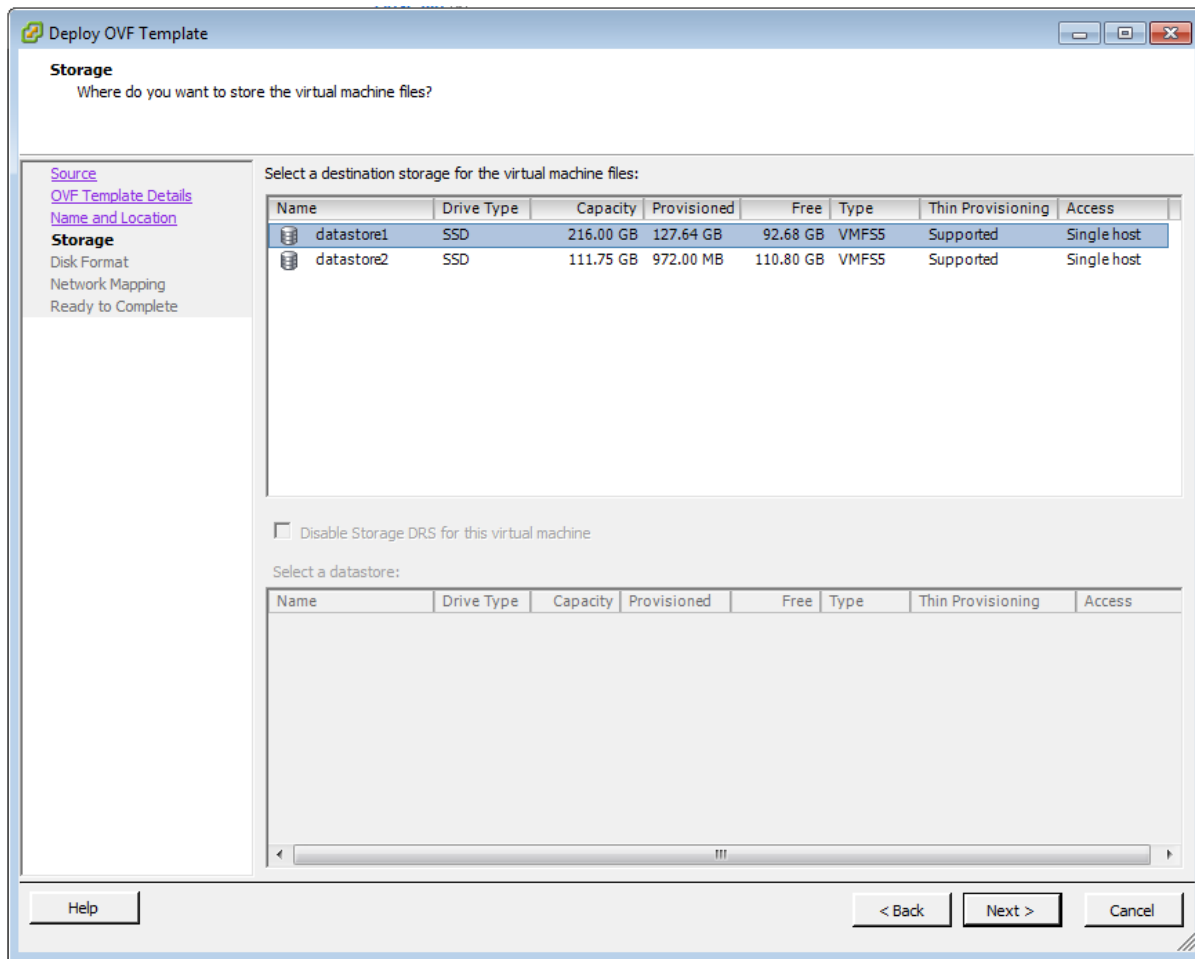
Name and Location
Specify a name and location for the deployed template

[Source](#)
[OVF Template Details](#)
Name and Location
Storage
Disk Format
Network Mapping
Ready to Complete

Name:
awingu-VM
The name can contain up to 80 characters and it must be unique within the inventory folder.

Help < Back Next > Cancel

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



7. Select "Thin provision"

Deploy OVF Template

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

[Source](#)
[OVF Template Details](#)
[Name and Location](#)
[Storage](#)
Disk Format
[Network Mapping](#)
Ready to Complete

Datastore:

Available space (GB):

☐ Thick Provision Lazy Zeroed
☐ Thick Provision Eager Zeroed
☒ Thin Provision

[Help](#) [< Back](#) [Next >](#) [Cancel](#)

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

Deploy OVF Template

Network Mapping
What networks should the deployed template use?

[Source](#)
[OVF Template Details](#)
[Name and Location](#)
[Storage](#)
[Disk Format](#)
Network Mapping
Ready to Complete

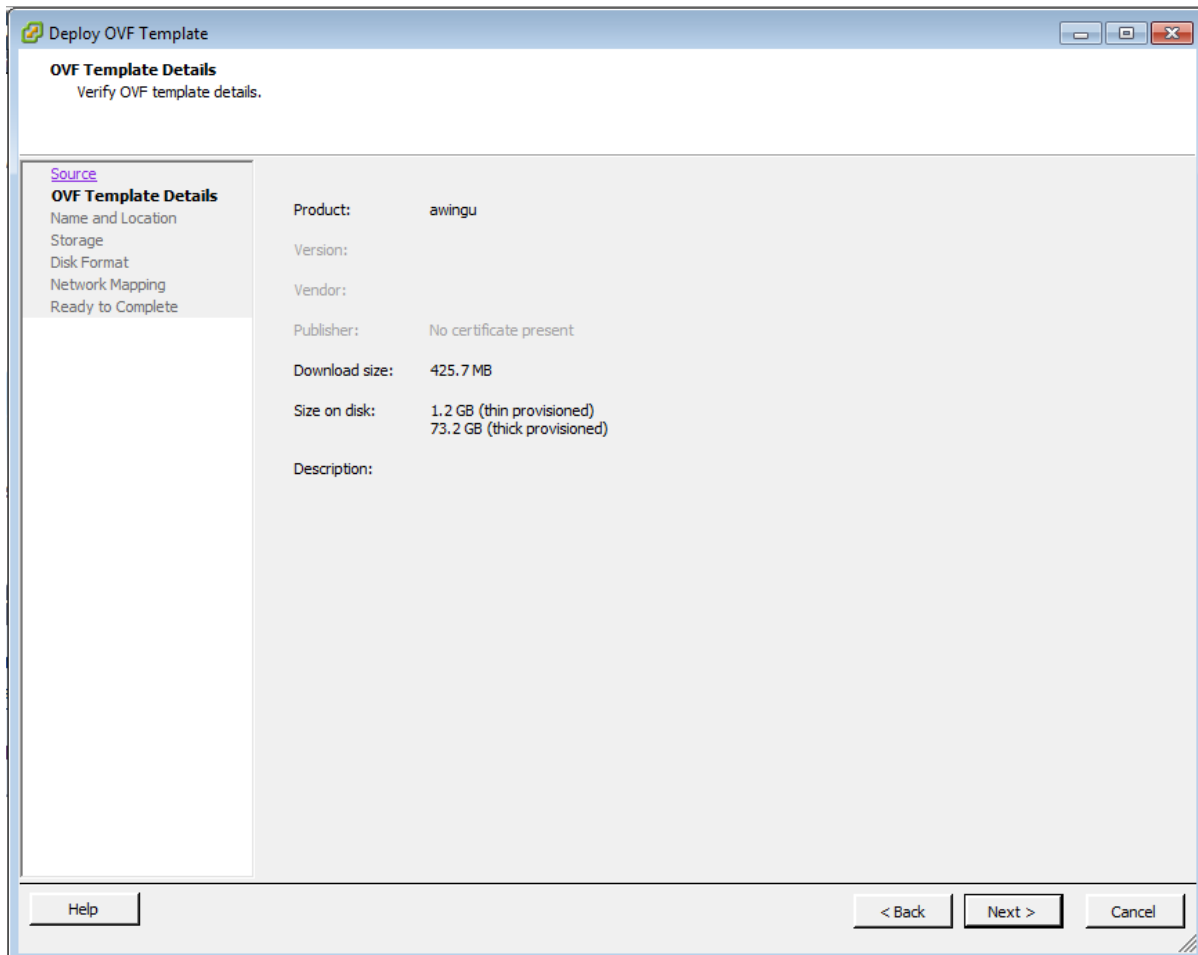
Map the networks used in this OVF template to networks in your inventory

Source Networks	Destination Networks
bridged	VM Network

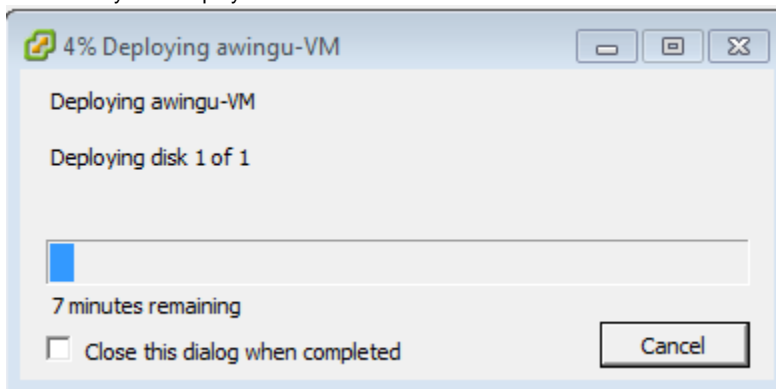
Description:
The bridged network

Help < Back Next > Cancel

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

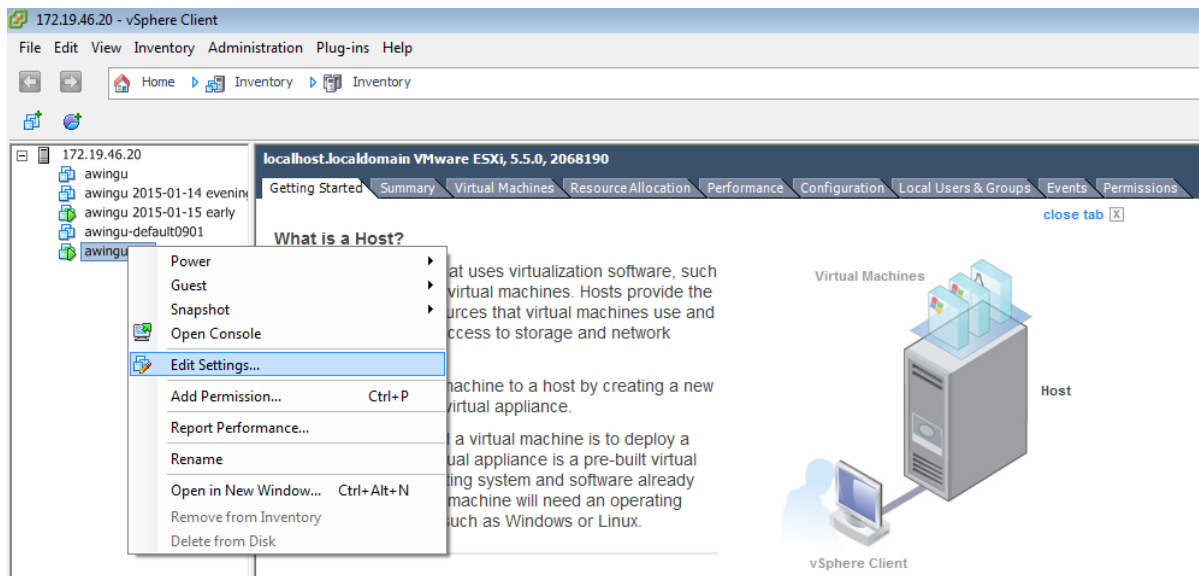


10. Click finish to start download and deploy the Awingu appliance. This step may take several minutes. Do **not** start the machine automatically after deployment.

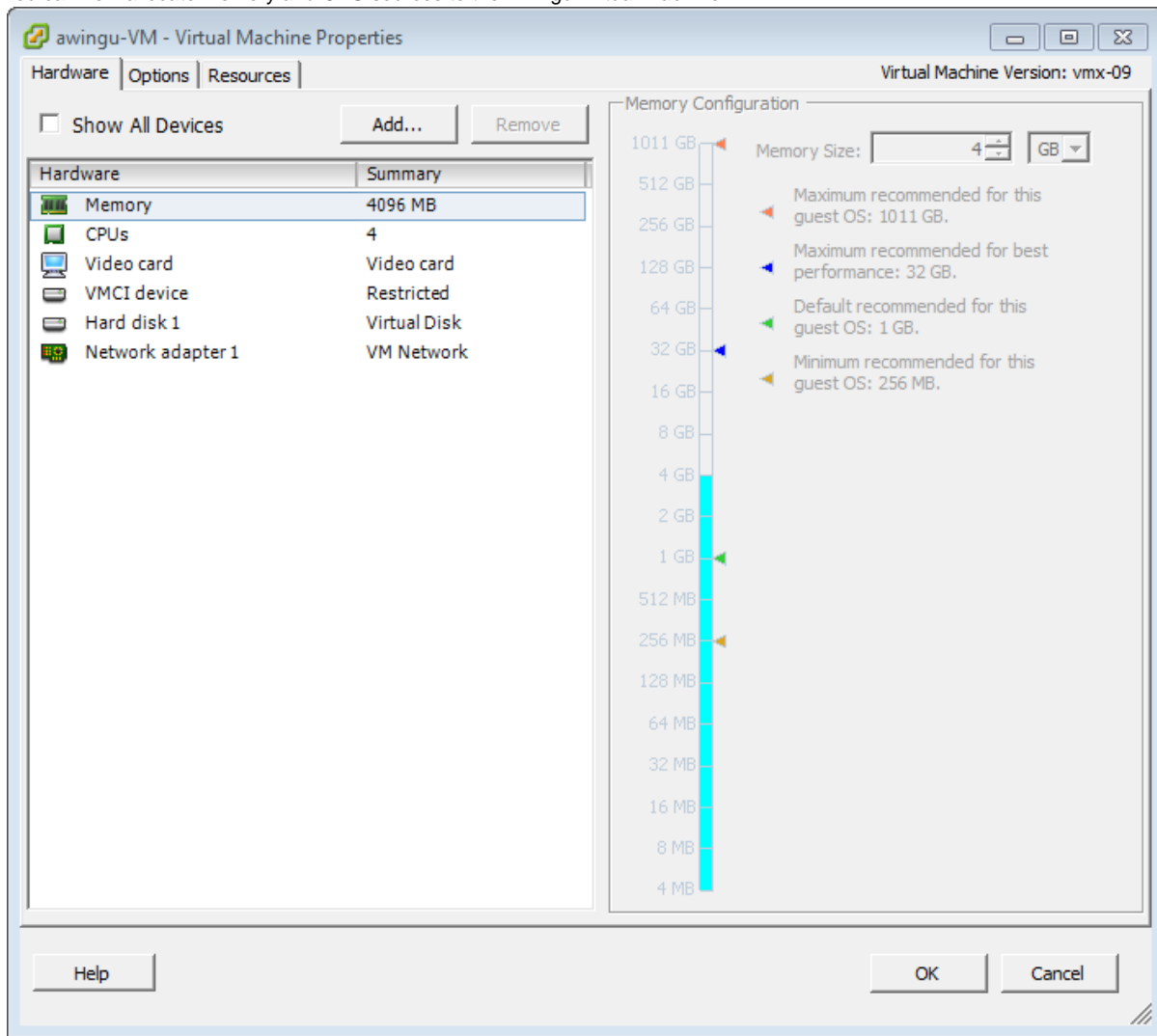


Step 2 - Configure your Awingu virtual machine settings

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



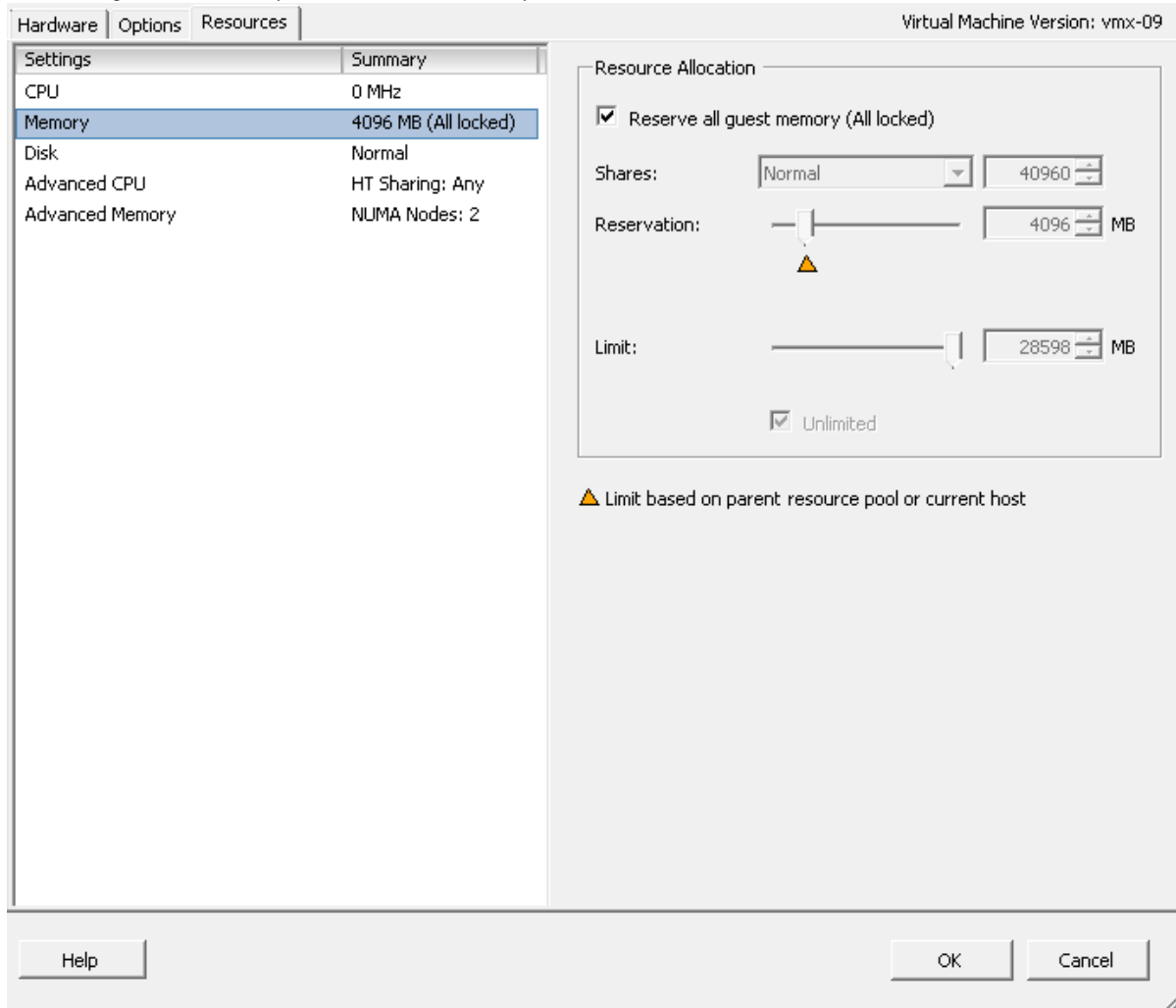
2. You can now allocate memory and CPU sources to the Awingu Virtual Machine



Awingu recommends the following specs for your virtual machine. Those specs are based on carefully performed internal load tests.

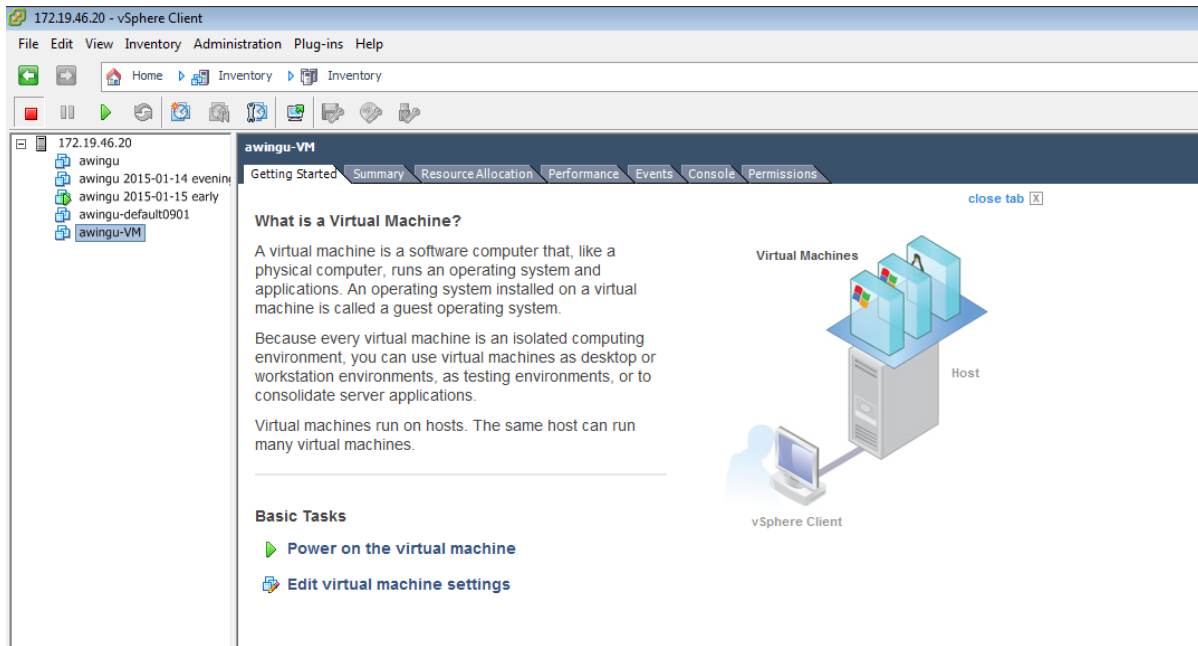
Number users	RAM	CPUs
20 concurrent users	4096 MiB	2 CPUs
50 concurrent users	4096 MiB	4 CPUs
100 concurrent users	8192 MiB	8 CPUs

- 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:

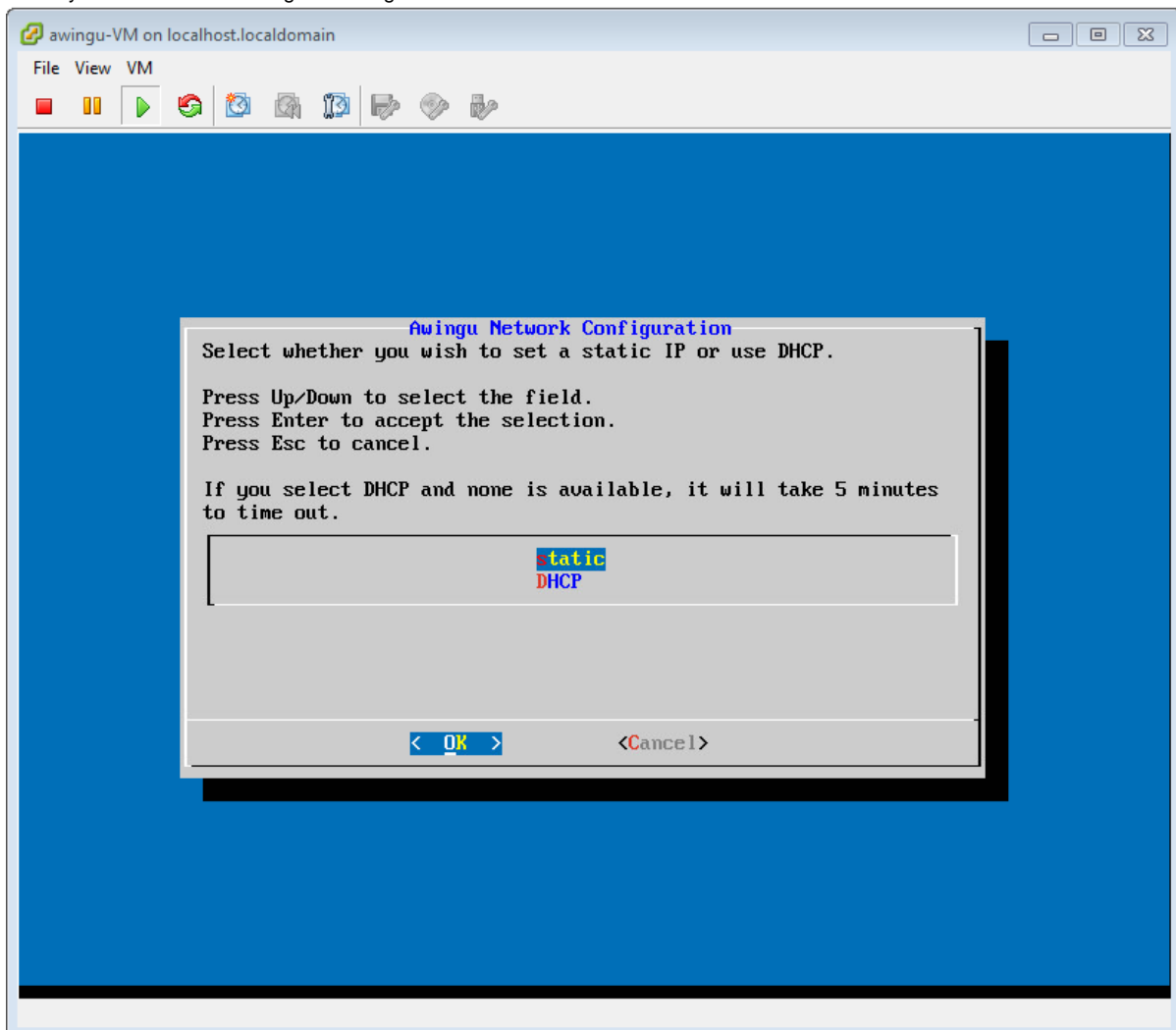


Step 3 - Start up your Awingu virtual machine

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



- 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:



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](#).

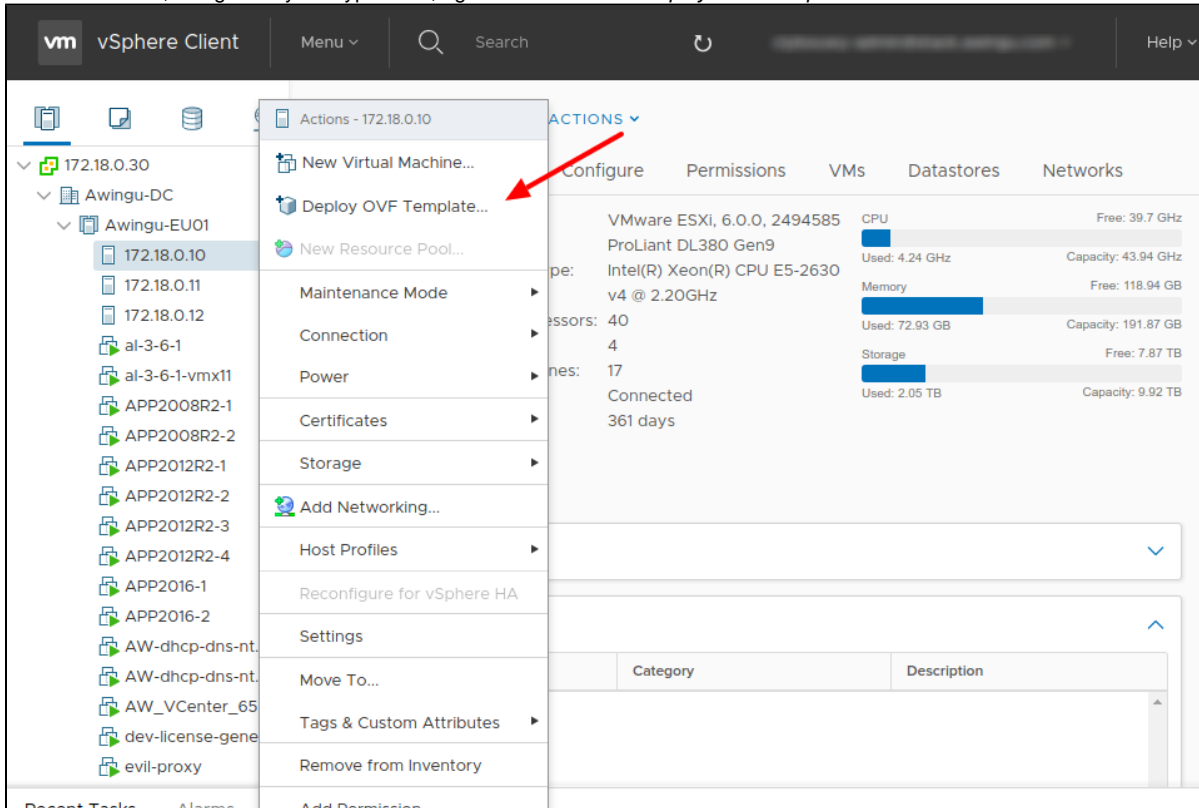
Deployment on VMware ESXi with vSphere Web Client

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

No file chosen

CANCEL
BACK
NEXT

- 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.

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 a name and folder

Specify a unique name and target location

Virtual machine name:

Select a location for the virtual machine.

172.18.0.30

> Awingu-DC

CANCEL
BACK
NEXT

5. Select the hypervisor to deploy on.

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 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.

CANCEL

BACK

NEXT

6. Review the details.

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

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)

CANCEL

BACK

NEXT

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.

CANCEL

BACK

NEXT

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

CANCEL

BACK

NEXT

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.

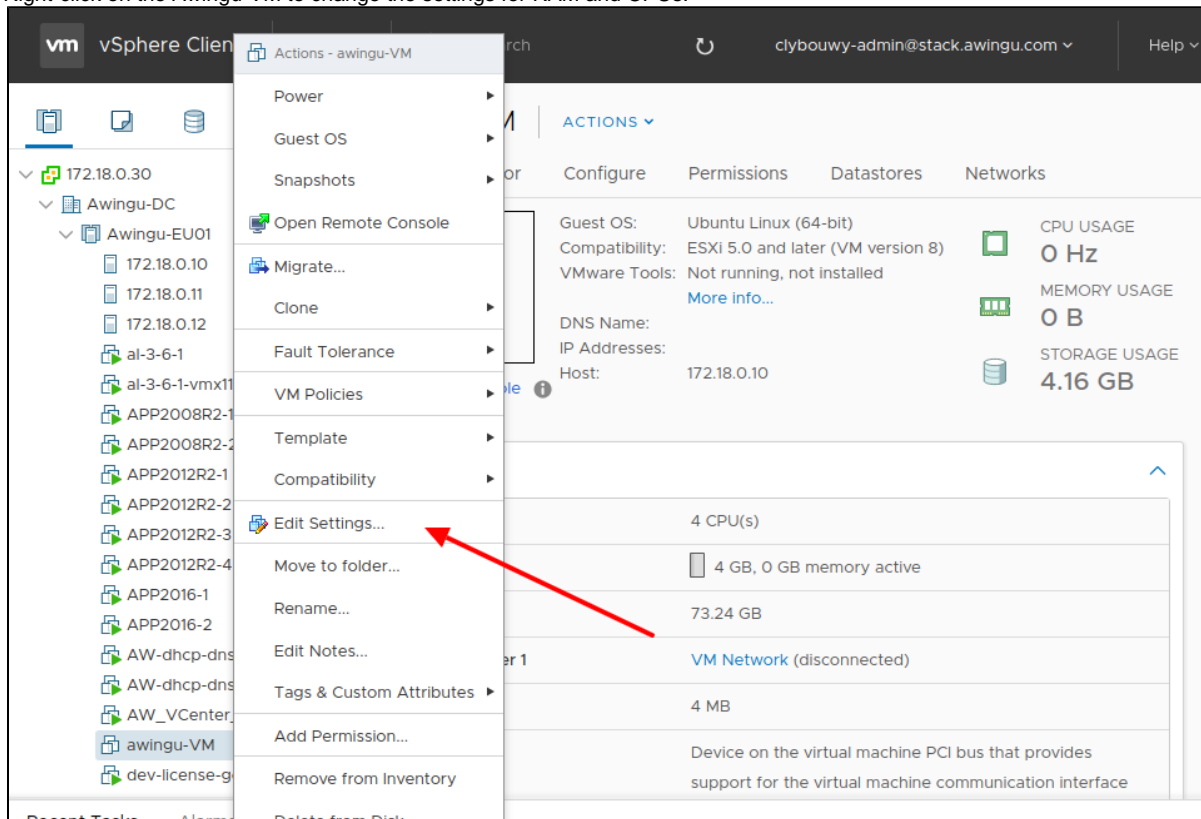
Provisioning type	Deploy OVF From Remote URL
Name	awingu-VM
Template name	awingu_vmx8
Folder	Awingu-DC
Resource	172.18.0.10
Location	ESX1-Storage

CANCEL
BACK
FINISH

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:



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

Number users	RAM	CPUs
20 concurrent users	4096 MiB	2 CPUs
50 concurrent users	4096 MiB	4 CPUs
100 concurrent users	8192 MiB	8 CPUs

For more details, see [Sizing 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.

Edit Settings | awingu-VM

Virtual Hardware | VM Options

ADD NEW DEVICE

> 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

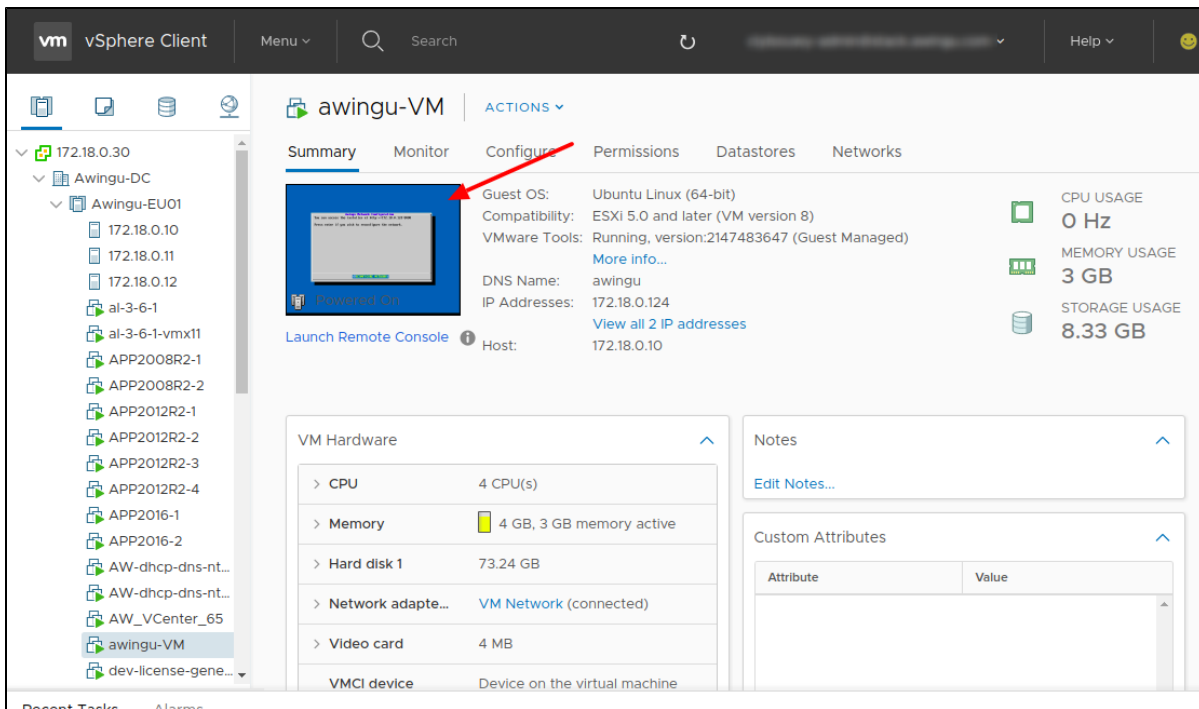
Additional Hardware

CANCEL

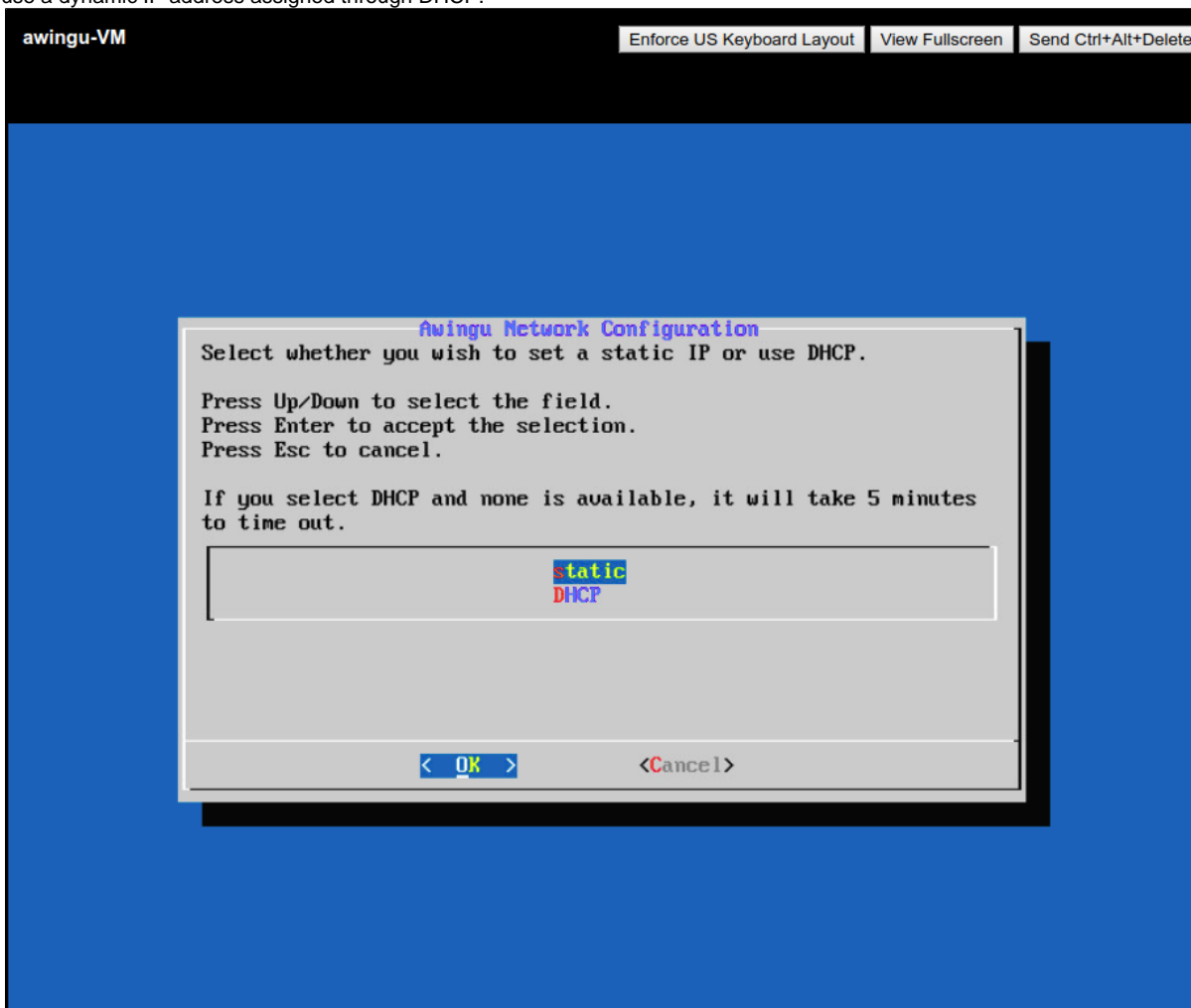
OK

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.



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.



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 awingu 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 follows:

```
# on debian-based systems
sudo apt-get install qemu-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 with 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:

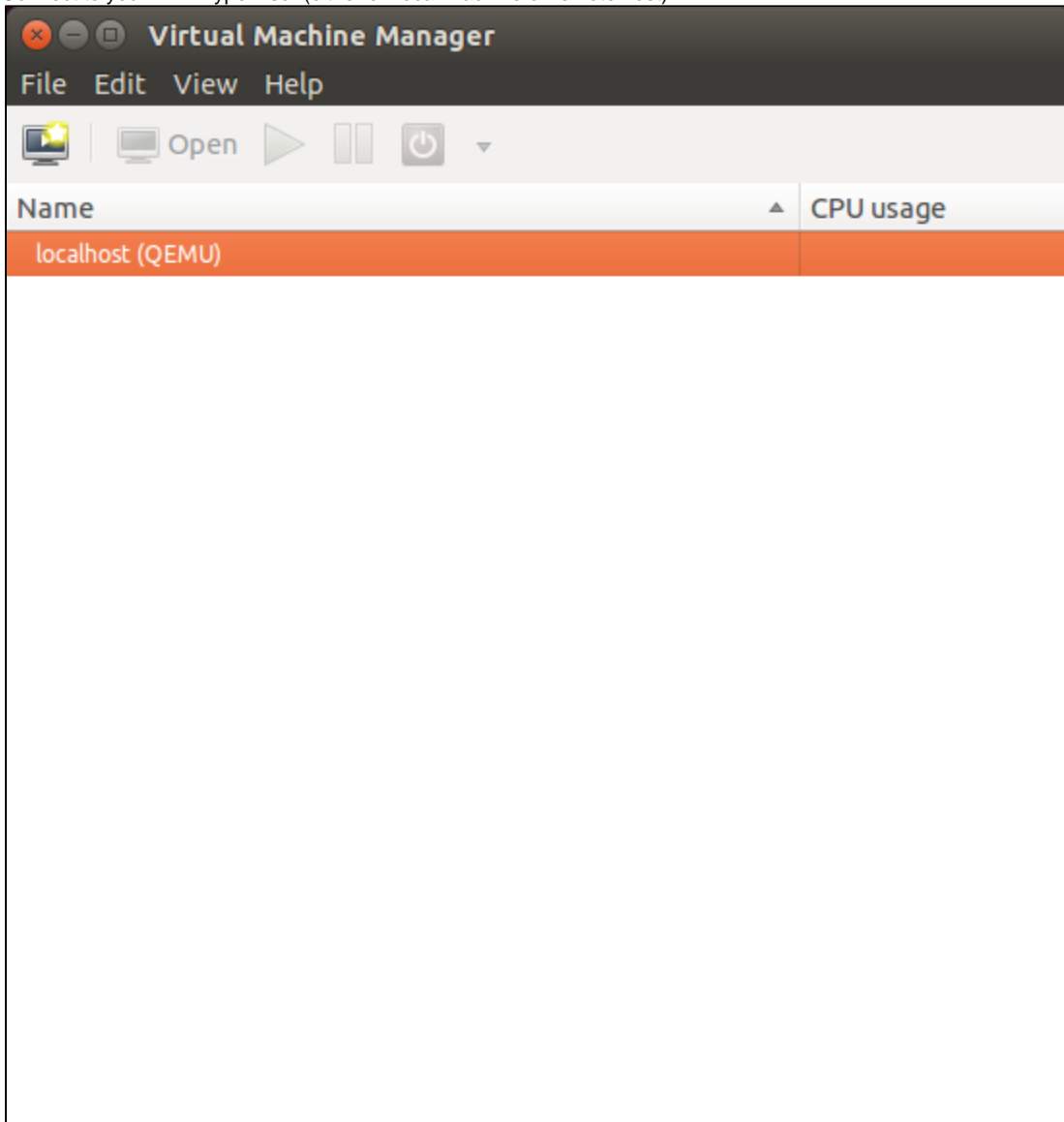
```
# on debian-based systems
sudo apt-get install virt-manager

# 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.

New VM

Create a new virtual machine
Step 1 of 4

Enter your virtual machine details

Name:

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 use the same import settings.

New VM

Create a new virtual machine
Step 2 of 4

Provide the existing storage path:

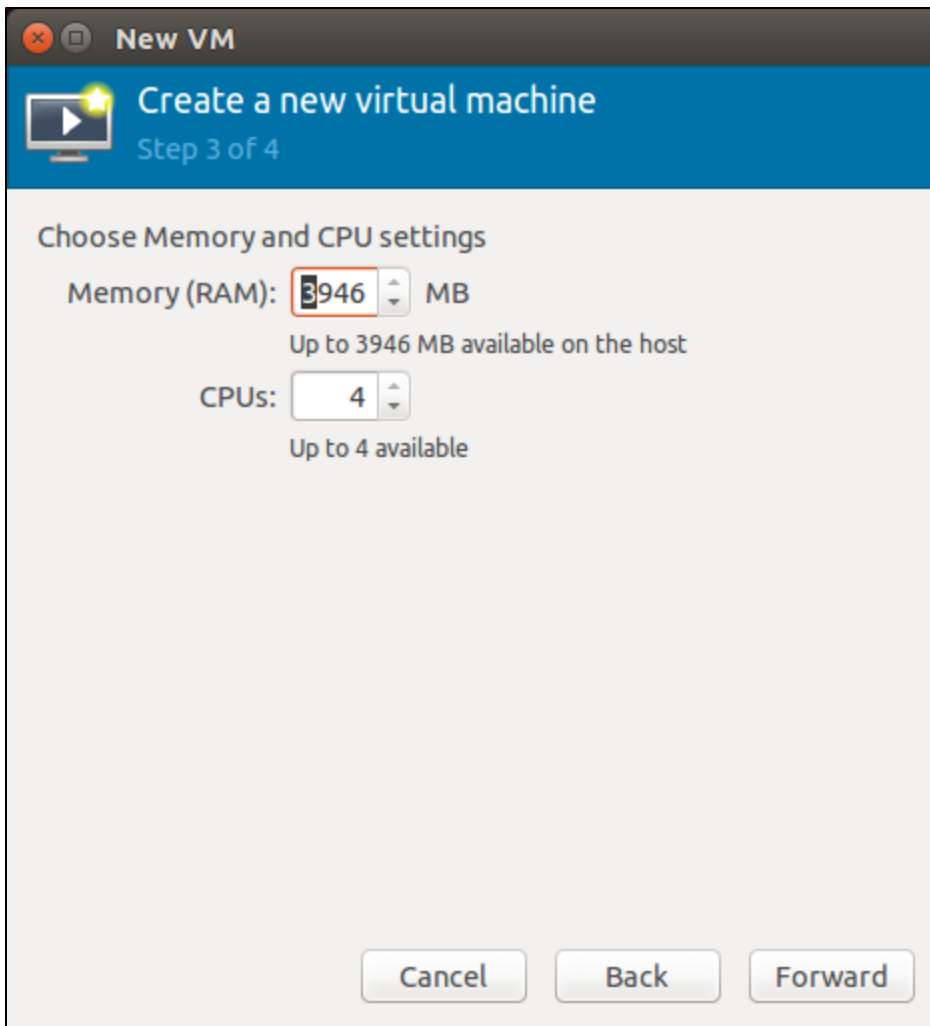
Choose an operating system type and version

OS type:

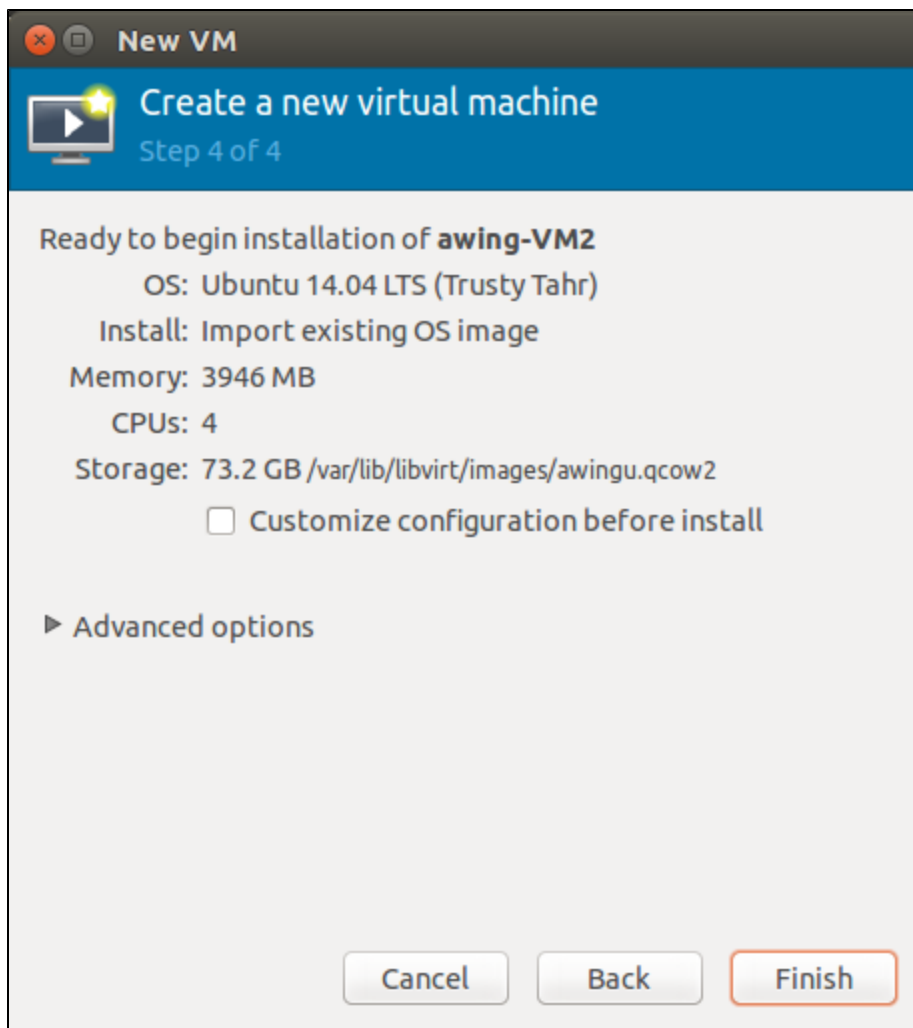
Version:

6. Specify RAM and CPU settings for your VM:

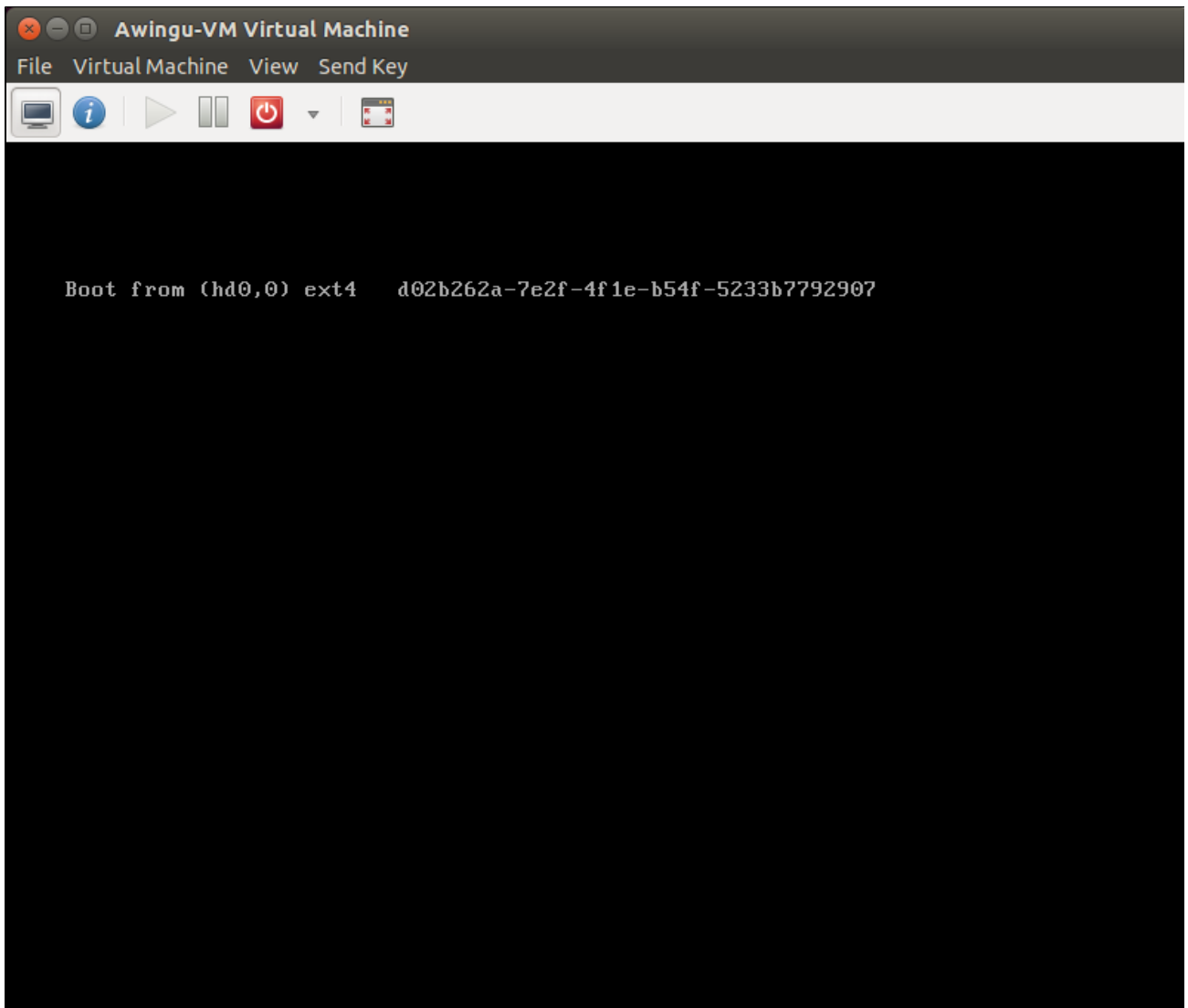
Number users	RAM	CPUs
20 concurrent users	4096 MiB	2 CPUs
50 concurrent users	4096 MiB	4 CPUs
100 concurrent users	8192 MiB	8 CPUs



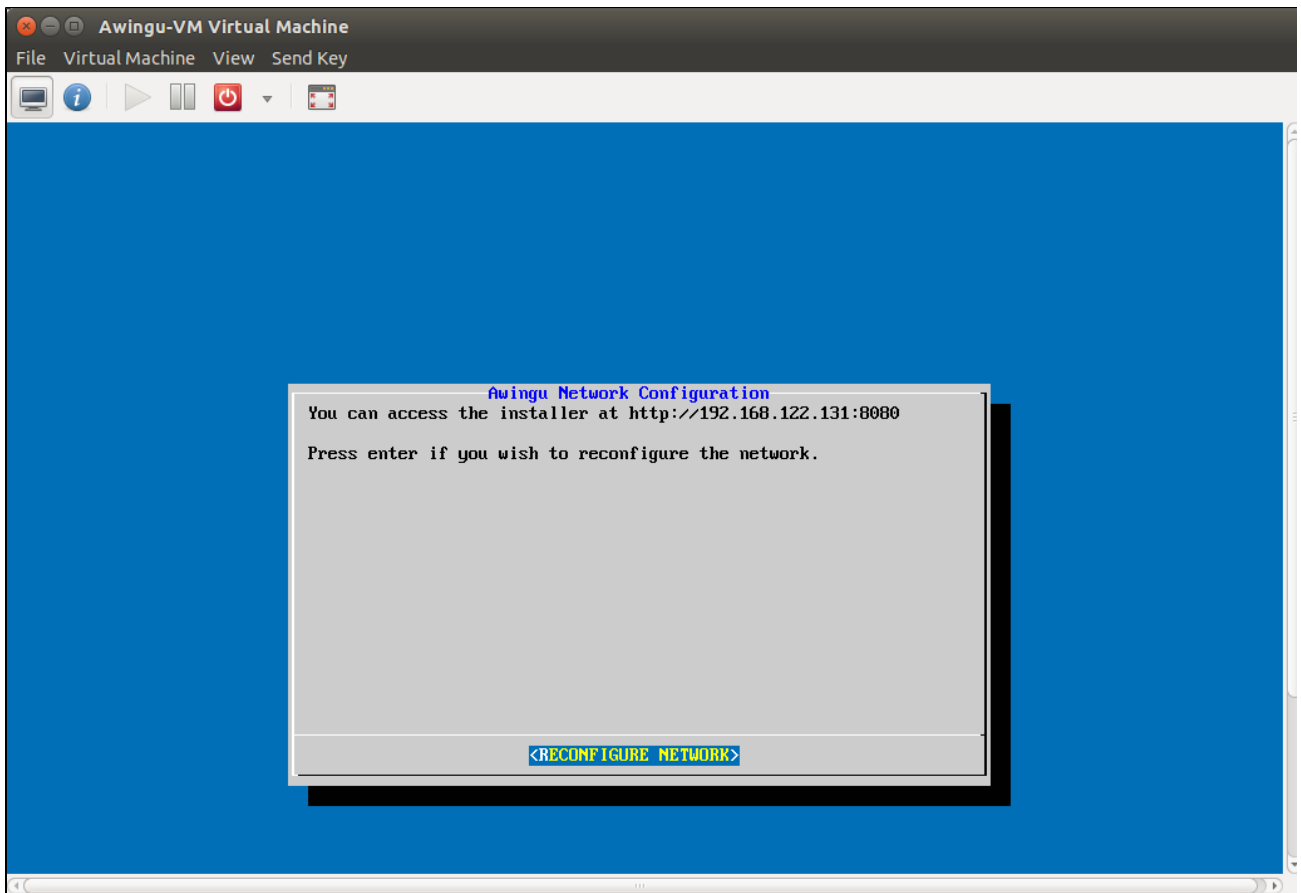
7. Review your virtual machine settings. You don't need to change the advanced options.



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



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.



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](#).

Deployment on Microsoft Azure

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

Deploying using the Azure Classic Portal

The SAS URL is provided on: <http://repo-pub.awingu.com/appliances/latest/azure/>

Deployment on Amazon EC2

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

Deployment on Google Compute

Request access by sending google id (email) to support@awingu.com

Awingu Installer

- Accessing the installer
- Step 1 - End User License Agreement
- Step 2 - Setup Management User
- Step 3 - Server Configuration
- Step 4 - Database Configuration
- Step 5 - Summary
- Installation Progress
- Install complete

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 from 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.**

Previous

Next

Finish

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

A PDF version of the EULA can 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

Previous

Next

Finish

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 Configuration3/5

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

Previous

Next

Finish

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

i 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 databases

Frontend Web

E.g.: `mysql://username:password@example.com:3306/frontendWeb`

Graphite Web

E.g.: `mysql://username:password@example.com:3306/graphiteWeb`

Previous

Next

Finish

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.

Externalizing a internal database after installation is not possible.

Changing the database connection URLs after installation is not possible.

Awingu provides connectors for *Microsoft SQL (both on-premise as Azure SQL Database)* and *PostgreSQL*.

We need two databases for Awingu: **Frontend Web** and **Graphite Web**. Each database is specified with a *Connection URL* adherent to following structure:

`protocol://username:password@server:port/database`

Where **protocol** should be replaced by one of the following: `mssql` or `postgres`.

The server can be defined with its Fully Qualified Domain Name (FQDN) or its IPv4 address.

In case of MS SQL named instances, "server:port" can be replaced with "server\named_instance".

Please make sure the specified accounts and databases are available before proceeding.

Database credentials, name and host can contain following characters:

- a-z
- A-Z
- 0-9
- - _

Note that this means that for MS SQL, you cannot use domain users (e.g. DOMAIN\username) because they contain a backslash.

Below some **sample** URLs:

- **Frontend Web:** `postgres://username:password@database.company.com:5432/frontendweb`
- **Graphite Web:** `mssql://username:password@database.company.com\awingu/graphiteweb`

If all of the above is populated correctly, click **Next**. The connections to the databases will be verified by creating, editing and deleting a table in

each database. We also check if the databases are not already in use by Awingu.

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

Previous

Next

Finish

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

Installation Progress

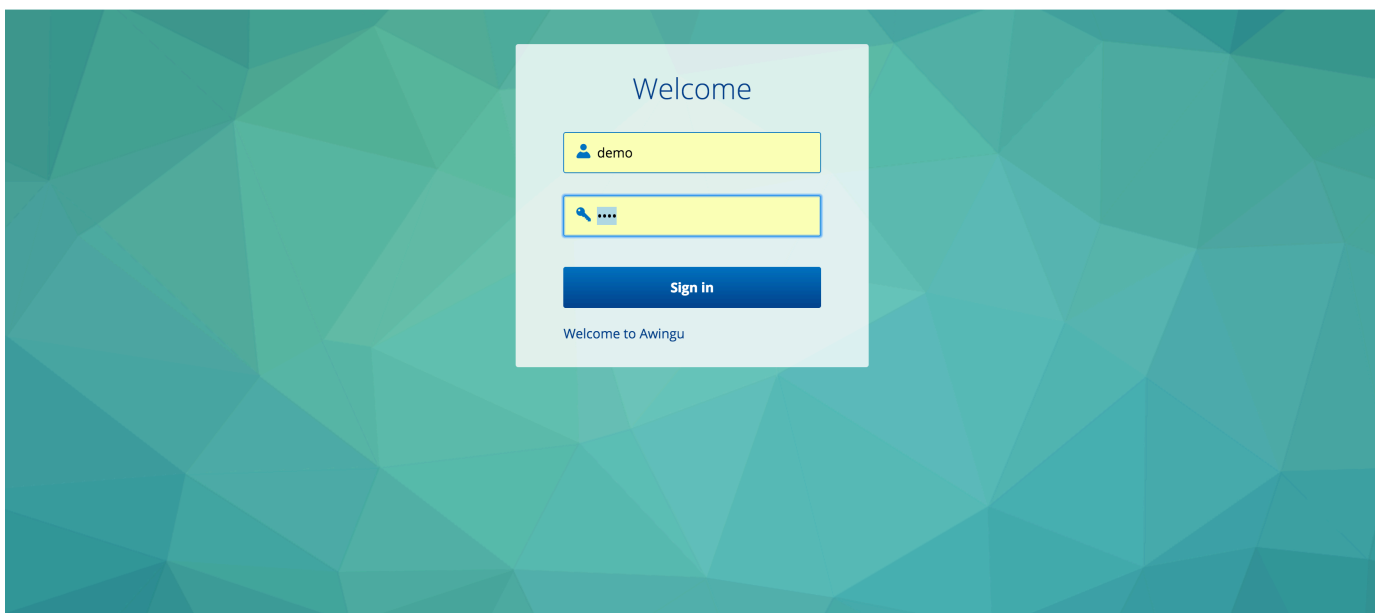
The Awingu appliance is *installing packages*.

This operation will take *approximately 15 min*.

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

Install complete

Awingu.com
Cloud Managed BY Device Appliance



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 be able to use an AD user in the admin group to login to Awingu, which is recommended.

Azure Awingu All-In-One

- Introduction
- Deployment
 - Basics
 - Awingu Configuration
 - Windows Backend Configuration
 - Summary
- Next Steps

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

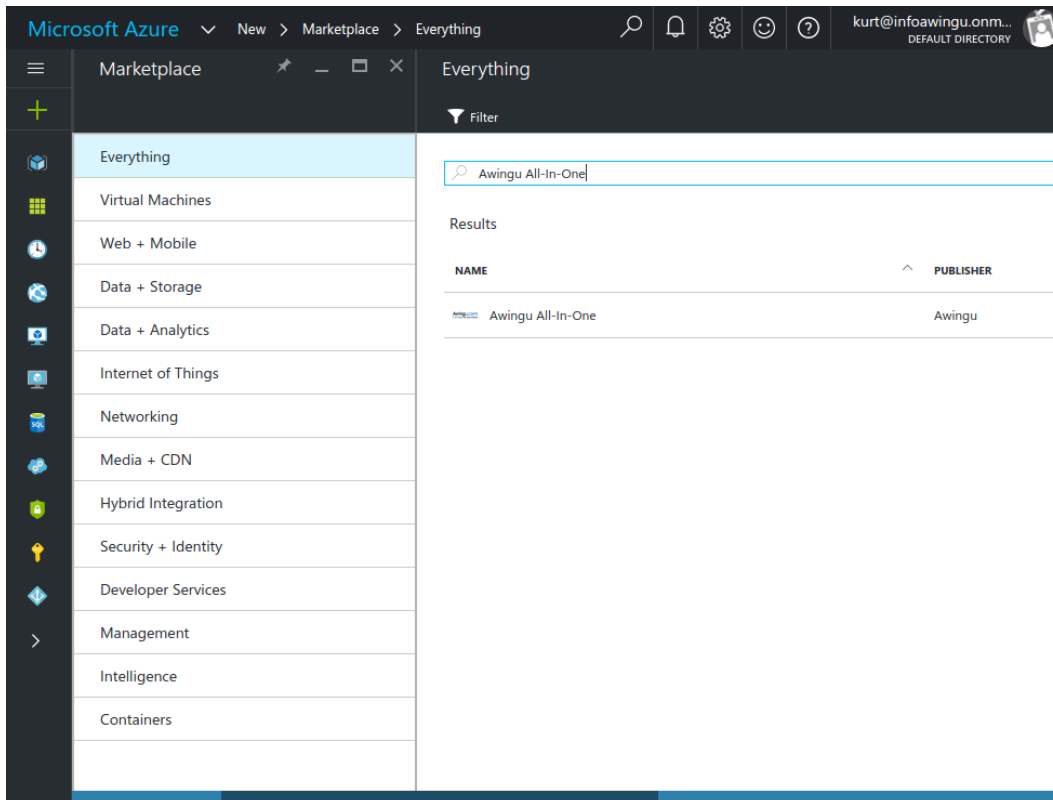
Deployment

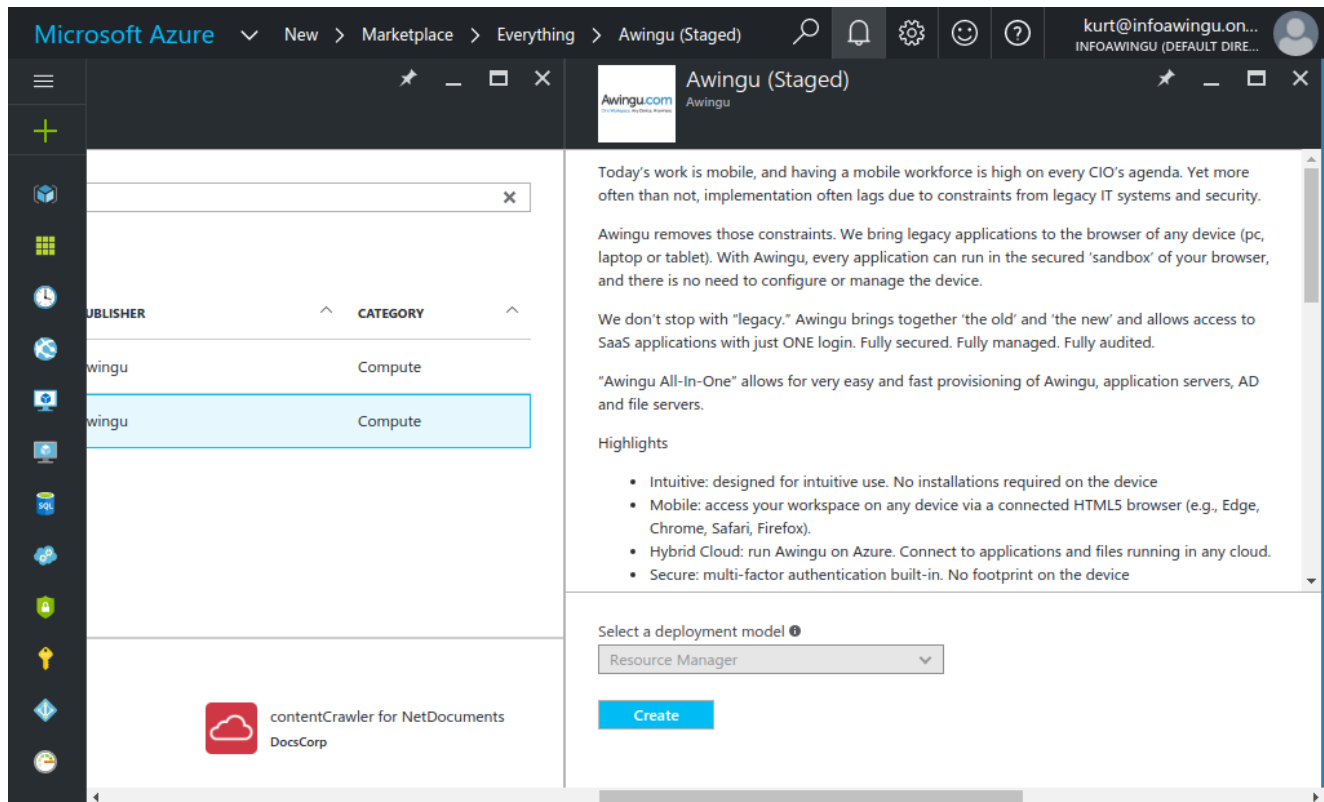
Deploying an *Awingu All-In-One* Azure marketplace solution is done through the Azure Portal using a wizard in 3 easy steps.

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.





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

Create Awingu (Staged) Basics

- 1 Basics
Configure basic settings
- 2 Awingu
Configure Awingu
- 3 Windows Backend
Configure Windows Backend
- 4 Summary
Awingu (Staged)
- 5 Buy

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

Create Awingu (Staged) Awingu Configuration

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

* 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.

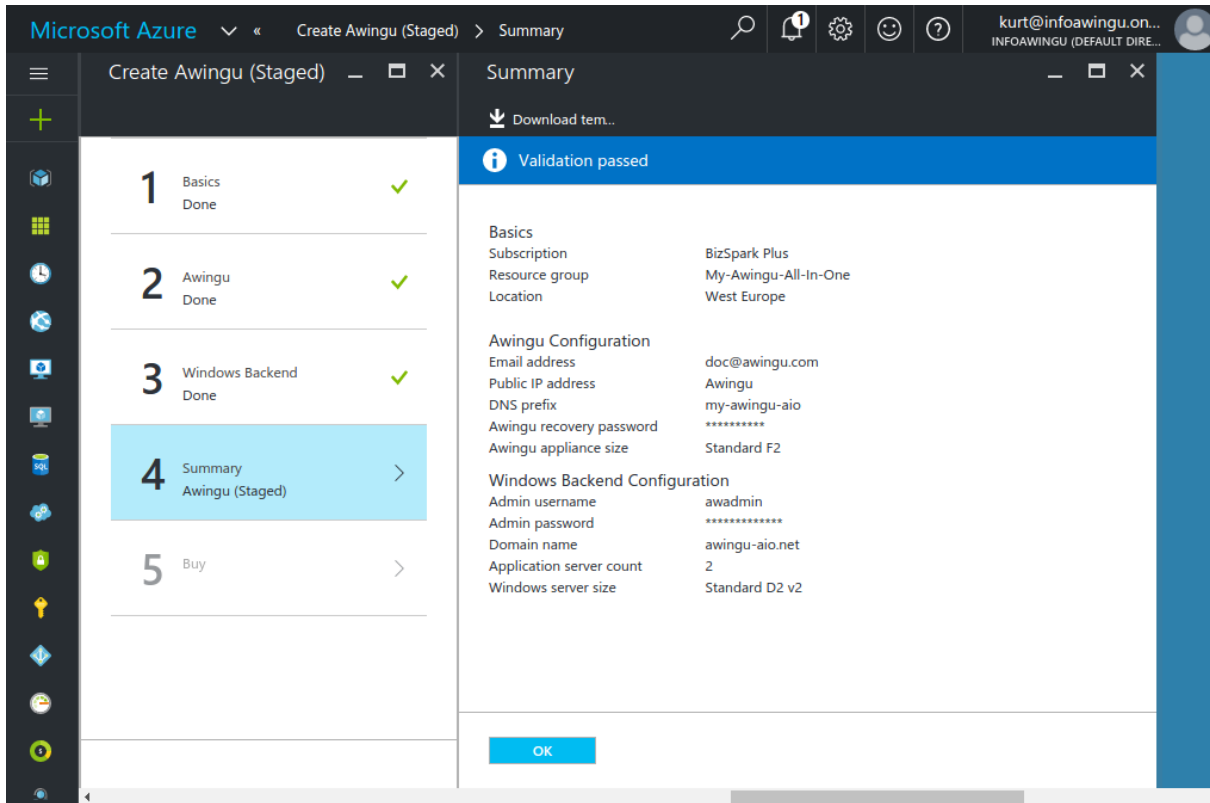
This backend will consist of 1 Active Directory server and a selectable amount of Windows application servers. The Awingu appliance will be configured automatically to connect to these servers.

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 server size	Azure appliance size to use for all Windows servers.

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.



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](#)
- [Multi-tenancy](#)

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 be able to use an AD user in the admin group to login to Awingu, which is recommended.

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.

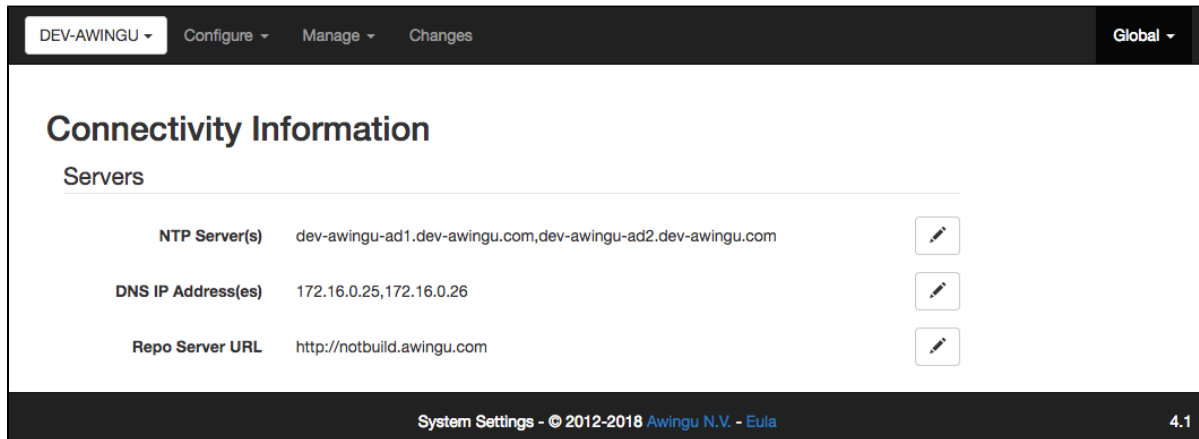
- [Connectivity Settings](#)
- [General Information](#)
- [Service Management Settings](#)
- [Domain Settings](#)
- [Certificate Settings](#)
- [Troubleshoot](#)

Connectivity Settings

- Servers
- HTTP Proxy
- External Reverse Proxy
- SNMP
- Direct TCP (Use SMB/CIFS via port 445)
- SSL Offloader
- Database connection URLs
- Database Backup SFTP user

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

Servers

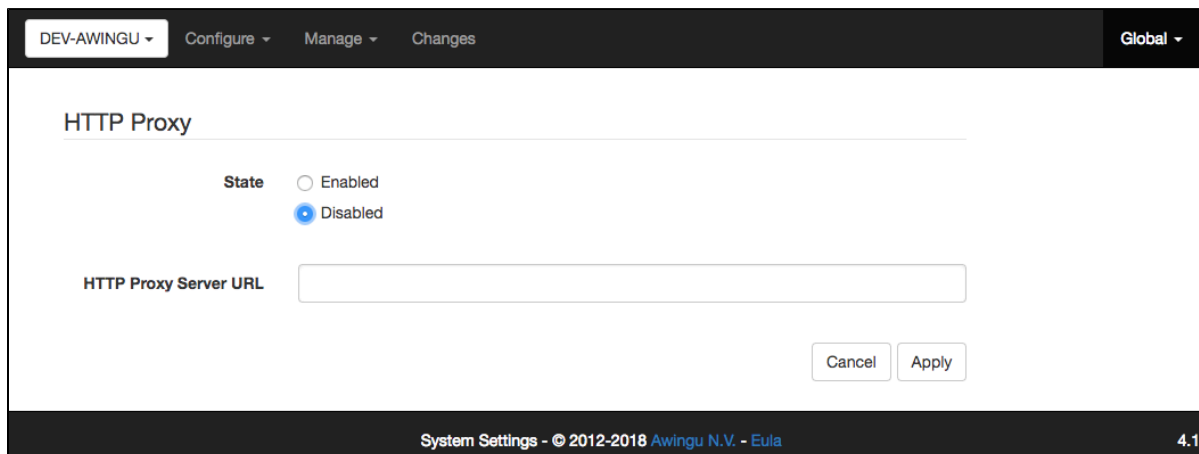


The screenshot shows the 'Connectivity Information' page in the Awingu interface. The 'Servers' section is active, displaying three configuration items: 'NTP Server(s)' with the value 'dev-awingu-ad1.dev-awingu.com,dev-awingu-ad2.dev-awingu.com', 'DNS IP Address(es)' with '172.16.0.25,172.16.0.26', and 'Repo Server URL' with 'http://notbuild.awingu.com'. Each item has an edit icon to its right. The top navigation bar includes 'DEV-AWINGU', 'Configure', 'Manage', 'Changes', and 'Global'. The footer shows 'System Settings - © 2012-2018 Awingu N.V. - Eula' and the version '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



The screenshot shows the 'HTTP Proxy' configuration page. It features a 'State' section with two radio buttons: 'Enabled' and 'Disabled', with 'Disabled' selected. Below this is a text input field for 'HTTP Proxy Server URL'. At the bottom right are 'Cancel' and 'Apply' buttons. The top navigation bar is identical to the previous screenshot. The footer shows 'System Settings - © 2012-2018 Awingu N.V. - Eula' and the version '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, Skype for Business 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

DEV-AWINGU ▾ Configure ▾ Manage ▾ Changes Global ▾

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.

Cancel Apply

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


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

DEV-AWINGU ▾ Configure ▾ Manage ▾ Changes Global ▾

SNMP

State Enabled 

Password *****

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

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*.

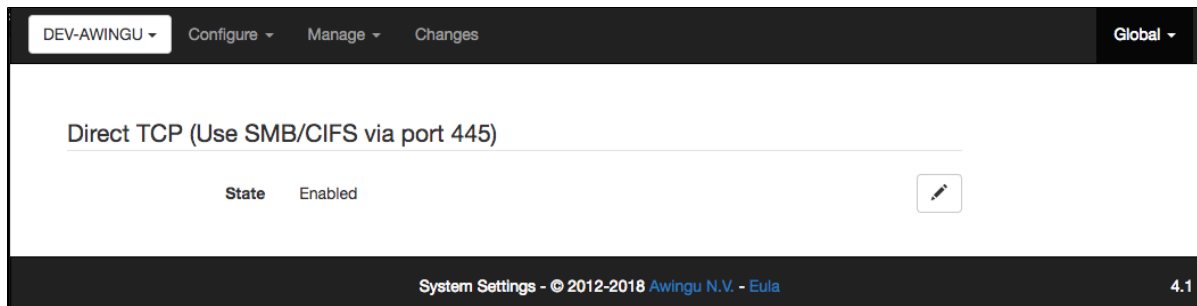
The agents are accessible on *UDP port 161* with the read-only user *awingu*.

- **State:** Enable or Disable SNMP agents on the Awingu appliance(s)
- **Password:** Self-selected password for read-only user *awingu* required to access the SNMP agents

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

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

Direct TCP (Use SMB/CIFS via port 445)

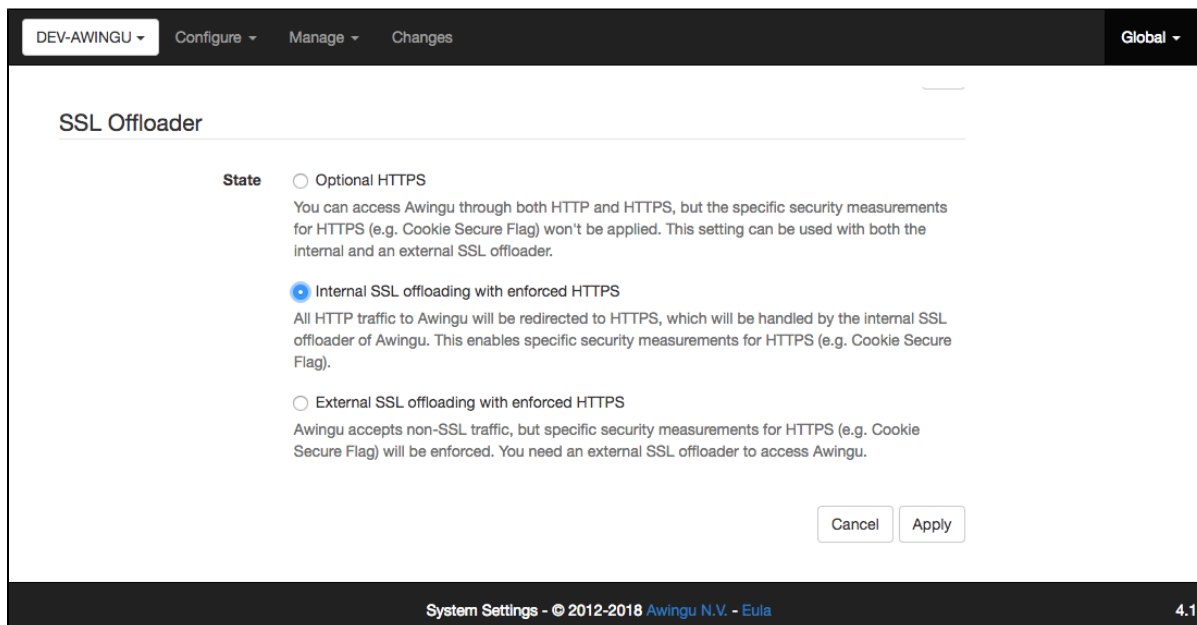


This settings specifies the SMB/CIFS ports used:

- Enabled: UDP port 137, TCP port 445 (default)
- Disabled: UDP port 137 broadcast, TCP port 139 (for older SMB servers)

Direct TCP should be enabled when accessing DFS namespaces and when using CIFS drives in a public cloud (where broadcasts are typically blocked).

SSL Offloader



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.

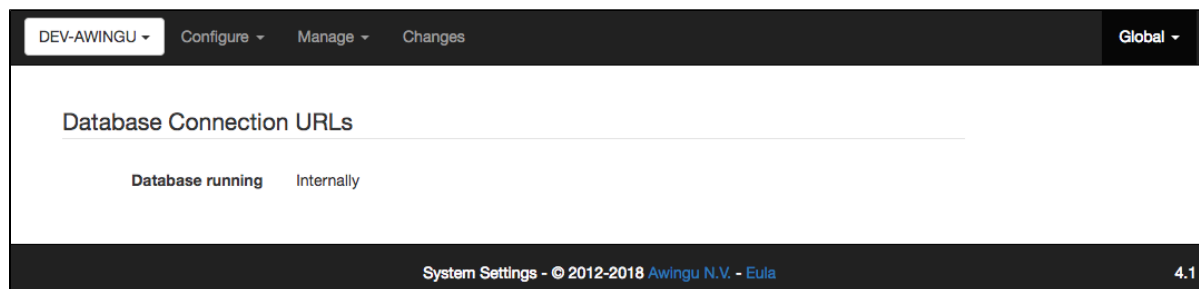
The internal SSL offloader can be used in three states:

- **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.

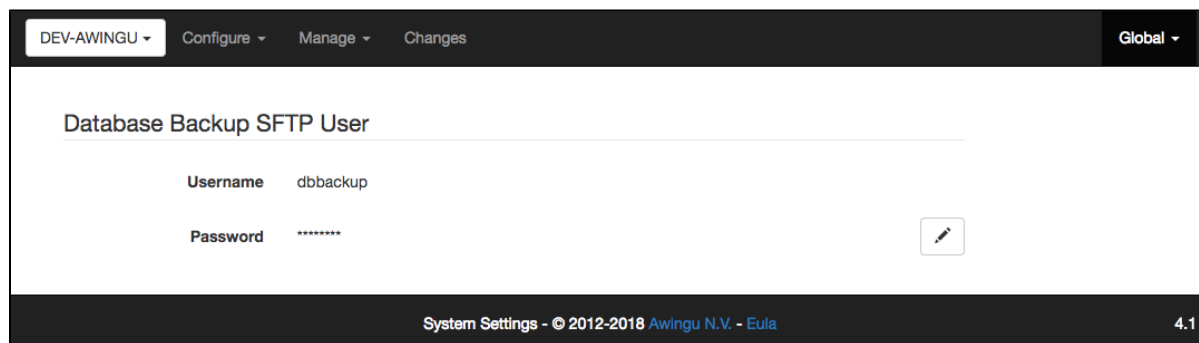
Note: if you switch back from HTTPS to HTTP, you will need to clear your browser cache and delete your Awingu cookies to be able to use Awingu again.

Database connection URLs



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

Database Backup SFTP user



This parameter is only relevant when the Awingu internal database is used. Awingu saves the database to local disk every day. You can retrieve this dump and saving it on another system via SFTP. The dumps 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.


General Information

- Management User
- Remote Support
- Partner
- Account Manager
- Anonymous Usage Reporting
- License
- Upgrade Version


DEV-AWINGU ▾ Configure ▾ Manage ▾ Changes Global ▾

General Information


Management User

Username	admin	
Whitelisted Subnets	Disabled	



Remote Support

Intervention Password	Disabled	
-----------------------	----------	---


Partner

Address	Mÿ cœl Åwingu Partnér Somewhere far -----> away Or somewhere \ near XOXO Gent Far East of Flanders Belgium +9876543210	
---------	---	---


Account Manager

Name	Mr. Account Manager	
Phone Number	+1234567890	

Anonymous Usage Reporting

State	Disabled	
-------	----------	---

License

Info	Awingu Type: License Terms: <ul style="list-style-type: none">• 1000 CONCURRENT users until 2021-12-31 Revision: 1	
------	--	---

Upgrade Version

Versions	<div></div>
----------	-------------

Could not fetch available versions from the repository server. Please make sure that the Repo Server URL on the Connectivity page is correct and that it is reachable from the Awingu appliance.

Upgrade

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.

Cancel

Confirm

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.

Close

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

Remote Support

Intervention Password

Enabled

Regenerate

Partner

Enter the contact details of the **Awingu 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 **Awingu partner**.

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

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.

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.

- There is maximum number of concurrent Awingu users allowed by this license. A concurrent user is defined as a concurrent browser connected to Awingu. Hence, one user connecting to Awingu from 2 different devices will be counted as two concurrent users. When the concurrent user limit is reached, new users will not be able to connect to Awingu for as long as other users do not first disconnect.
- There is an expiration date of the license. Beyond the expiration date, no end-user will be able to access Awingu.

Awingu can be used with 2 concurrent users for 60 days when no (valid) license is present.

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

Upgrade Version

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

Service Management Settings

- [Introduction](#)
- [Adding Awingu appliances](#)
- [Removing an Awingu appliance](#)
- [Assigning roles](#)

Introduction

Service Management enables you to add and remove Awingu appliances (nodes) to your environment and define the roles of each Awingu appliance.

The main page gives you an overview of all registered Awingu appliances and which roles are assigned to them.

Please refer to [Sizing Requirements](#) for supported multi node architectures.

Remarks

Once an appliance has been added and configured, **you cannot change its IP address**. Doing so will result in services failing.

STACK ▾

Configure ▾

Manage ▾

Changes

Global ▾

Service Management

i Changes are not allowed when there are unapplied changes.

Appliances can only be deleted if no service are assigned to it.

The database service cannot be moved when an internal database is used.

☐ Advanced Mode

Hostname	IP address	Backend	Database	Frontend
long-living-m-v2-4-0-no...	10.147.128.122	✓	✓	✓
long-living-m-v2-4-0-no...	10.147.128.121			✓

System Settings - © 2012-2018 [Awingu N.V.](#) - [Eula](#) 4.0.2

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, UDP 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](#)
- [Domains](#)
- [Default Domain](#)

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

DEV-AWINGU ▾









Configure ▾

Manage ▾

Global ▾

Domains

Bulk Action ▾

✓	Name ▲	NetBIOS Name	FQDN for UPN	Administrativ...	Is Default	Actions
✓	DEV-AWINGU	DEV-AWINGU	dev-awingu.com	✓	✓	<div>Set default</div> <div> </div>
✓	DEV-AWINGU-2	DEV-AWINGU	dev-awingu.com			<div>Set default</div> <div> </div>
✓	OU1	STACK	stack.awingu.c...			<div>Set default</div> <div> </div>
✓	STACK	STACK	stack.awingu.c...	✓		<div>Set default</div> <div> </div>

Items per page 10 ▾

⏮

⏪

1 ▾

/ 1

⏩

⏭

Add

System Management Console - © 2012-2017 Awingu N.V. - [Eula](#) 3.5.0

DEV-AWINGU
Configure
Manage
Global

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	
Base DN	dc=dev-awingu,dc=com	
LDAP over SSL?	Enabled	
DNS Server	172.16.0.25	
Bind user for domain	binduser	
Password for bind user	*****	
Create Bind Name	builtin.create_domain_bind_name	
Find Groups	builtin.find_groups_by_member_of	
Max Concurrent Users	Disabled	

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

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 counterpart when logging in using the user's UPN. Used to sign in with e-mail address like user name. 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

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 Concurrent Users:** If enabled, you can configure the maximum number of users that can concurrently login on this Awingu 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 compliance.

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 Name:** The username of the service account
- **Bind Password:** 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 (default): find group via memberOf field in LDAP result
 - builtin.find_groups_by_token_groups: find group recursively (method 1)
 - 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

- Introduction
- Uploading certificates manually
 - Certificates with passphrases
 - Converting PFX certificates
 - Certification Sign Requests (CSR) for new certificates
 - Self-Signed Certificates
- Generating certificates automatically
- Replacing and deleting certificates

DEV-AWINGU ▾ Configure ▾ Manage ▾ Global ▾

Certificates

Start typing to search Bulk Action ▾

✓ 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...		

Items per page 10 ▾

Add

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

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](#).

Uploading certificates manually

Click on Add and provide following information:

- **Certificate:** manual
- **SSL 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.

- **SSL Certificate Key:** The private key file associated with the certificate in **.key format**, ASCII file, starting with:

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

or

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

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 passphrase. 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
```

Converting PFX certificates

The Awingu appliance only supports unencrypted PEM & KEY files. If you have a PFX based certificate you can convert them with OpenSSL. If you are looking for Windows binaries for OpenSSL you can find them here: <http://gnuwin32.sourceforge.net/packages/openssl.htm>

```
openssl pkcs12 -in [yourfile.pfx] -nocerts -out [keyfile-encrypted.key]
openssl pkcs12 -in [yourfile.pfx] -clcerts -nokeys -out [certificate.crt]
```

Certification Sign Requests (CSR) for new certificates

Most certificate providers will request a CSR file to generate a Certificate. Awingu doesn't have at this stage a build in CSR generator but this is not a problem.

A CSR or Certificate Signing request is a block of encrypted text that contains information that will be included in your certificate such as your organization name, common name (domain name), locality, and country. It also contains the public key that will be included in your certificate. A private key is usually created at the same time that you create the CSR. A certificate authority will use a CSR to create your SSL certificate, but it does not need your private key. You need to keep your private key secret. The most secure way to generate an own CSR file is to use openssl:

```
openssl req -nodes -newkey rsa:2048 -sha256 -keyout example.key -out
example.csr
```

As an alternative you can also use online services like <https://csrgenerator.com/>

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 most easy ways to do this is to use <http://www.selfsignedcertificate.com/>

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.

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

- Database actions
- dig
- download-logs
- ldapsearch
- ping
- tcpscan
- traceroute
- udpscan
- uptime

DEV-AWINGU ▾

Configure ▾

Manage ▾

Changes

Global ▾

Troubleshoot

1. Select Action

Start typing to search

database-create-backup

database-list-backups

database-restore-backup

dig

download-logs

ldapsearch

ping

tcpscan

traceroute

Days ⓘ

7

2. Execute Action

Clear

Select

Execute

System Settings - © 2012-2018 Awingu N.V. - Eula4.0

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. In the arguments field, you can provide the maximum age (in number of days) of the log files. The default value is 7 days. 0 days is today and -1 means all log files.

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](#).

System Settings - Configure

Domain specific settings are configured here:

- [Branding Configuration](#)
- [Feature Configuration](#)
- [User Connector Configuration](#)

Branding Configuration

- [Multi-domain branding behavior](#)
- [Configuration options](#)
 - [General](#)
 - [Wide Logo](#)
 - [Square logo](#)
 - [Login Page](#)

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

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
- Smooth fonts (anti-aliasing) in streamed applications
- Show Shares on Files page
- Show Folders on Files page
- Allow to download files from the Files page
- Allow to upload files in the Files page
- Allow session sharing
- Allow in-app printing
- Allow to use the local clipboard








DEV-AWINGU ▾

Configure ▾

Manage ▾

Global ▾

Features

Name	Smooth fonts (anti-aliasing) in streamed applications	
User Labels	<div>all: </div>	
Name	Show Shares on Files page	
User Labels	<div>all: </div>	
Name	Show Folders on Files page	
User Labels	<div>all: </div>	
Name	Allow to download files from the Files page	
User Labels	<div>all: </div>	
Name	Allow to upload files in the Files page	
User Labels	<div>all: </div>	
Name	Allow session sharing	
User Labels	<div>all: </div>	
Name	Allow in-app printing	
User Labels	<div>all: </div>	



Behavior

All features listed here are applied to users based on labels:

- When the labels of a users matches one the labels set to a feature, the feature will be applied for that user.
- To enable a feature for all users of the domain, please attach the predefined *all:* label to that feature.
- To disable a feature for all users of the domain, please remove any labels from that feature.

To create custom labels and to find more information, please refer to [Label Management](#).

Smooth fonts (anti-aliasing) in streamed applications

Smooth fonts result in a better visualization of fonts shown in streamed applications, but result in a higher bandwidth for applications with a lot of text.

Show Shares on Files page

When disabled:

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

Show Folders on Files page

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

Allow to download files from the Files page

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

Allow to upload files in the Files page

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

Allow session sharing

When disabled, the feature to share application sessions with other users is disabled. This feature is accessible in a streamed app when clicking on the polygon and then on the ellipsis (...).

Allow in-app 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.

Allow to use the local clipboard

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

User Connector Configuration

- User Groups
- User Profile Defaults
- Advanced Authentication
 - Multi-factor Authentication
- API Token Based Authentication
- Reverse Proxy
- Skype for Business Online Integration
- SSO Identity Provider (IdP)
 - SSO Services
- Application Sessions
 - Application Recording
 - Session keep-alive

User Groups

DEV-AWINGU ▾

Configure ▾

Manage ▾

Global ▾

DEV-AWINGU / User Connector

User Groups

Sign in White List

Disabled

Name ▴	Sign In Whitelist	Admin	Staff	Record	
Awingu Admins Çœßøÿ #"/@&%*[]	✕	✓	✕	✕	
Recorded Users Çœßøÿ #"/@&%*[]	✕	✕	✕	✓	

Items per page 10 ▾

⏮

⏪

1

/ 1

⏩

⏭

System Management Console - © 2012-2017 Awingu N.V. - Eula3.6.1

In this section, you can define User Groups, named *security groups* on Windows Domain Controllers. Those groups can be used for 2 use cases:

- **White listing:**
 - Enabled: only user in groups marked as *Sign in Whitelist* can sign-in.
 - Disabled: everybody with valid credentials in the LDAP/AD of the domain can sign-in to Awingu. Note: OU restrictions can apply via the *Base DN* set in [Domain Settings](#).
- **Domain Roles:** Members of the defined user groups can be assigned one or more of following roles:
 - **Admin:** users belonging to groups that are assigned to the "admin:" label and have access to the System Settings, the Dashboard and the Recorded Session Player.
 - **Staff:** (label for future use)
 - **Record:** users belonging to groups that are assigned to the "record:" label and have all their streamed sessions recorded. The [recording feature](#) needs to be enabled.

Via [Application Management](#), [Drive Management](#) and [Feature Configuration](#), you can use the same labels to limit certain applications/drives/features to certain user groups. Note: other labels than admin/record/staff can be defined in [Label Management](#).

To define user groups, click on the on the pencil on the right of the table. A new page opens, with:

- **Add User Group:** Enter the name as defined on the LDAP/AD.

The security groups entered are case sensitive!

- Check boxes **Sign In Whitelist**, **Admin**, **Staff** and **Record**

User Profile Defaults

The screenshot shows the 'User Profile Defaults' configuration page. At the top, there is a dark navigation bar with 'DEV-AWINGU' selected, and 'Configure' and 'Manage' tabs. A 'Global' dropdown is on the right. The main content area has a title 'User Profile Defaults' and a table with three rows: 'Keyboard layout' set to 'English United States', 'Language' set to 'English', and 'Guided tours' set to 'Enabled'. Each row has an edit icon (pencil) to its right. A vertical scrollbar is on the right side of the table. At the bottom, a dark footer bar contains the text 'System Management Console - © 2012-2017 Awingu N.V. - Eula' and the version '3.5.0'.

User Profile Defaults	
Keyboard layout	English United States
Language	English
Guided tours	Enabled

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.

Please note that a user can always update his preferred keyboard layout and language on his/her profile page.

Advanced Authentication

Multi-factor Authentication

DEV-AWINGU
Configure
Manage
Global

Multi-factor Authentication

Mode
RADIUS

Servers
radius.awingu.com

Port
1812

Secret

LDAP Username Attribute
sAMAccountName

Cancel
Apply

Whitelisted Subnets
172.22.2.0/24

Cancel
Apply

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.

Cancel
Apply

System Management Console - © 2012-2017 Awingu N.V. - Eula
3.6.1

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.

- Counter based OTP (builtin):** Leverages the built-in counter based one-time-password (OTP) functionality
 - Device setup:** 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.
 Note to *not* to use "time based" authentication.
 When enabled, new users can set-up secure devices to generate a token via an app. (e.g. Google Authenticator), if not, only already configured users can log-in to Awingu.
 - 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.
- Azure MFA:** Token will be validated by Azure Multi-Factor Authentication using MFA server
 For more information: [Integrating Awingu with Azure MFA](#)
 - SDK url:** URL of the *Azure MFA Server Mobile App Web Service*
 - SDK username:** User name configured for the *Azure MFA Server Mobile App Web Service*
 - SDK password:** Password configured for the *Azure MFA Server Mobile App Web Service*
- 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
 The RADIUS server needs to be configured to not increase the counter for a failed attempt. For FreeRadius, this means adding no_increment_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\Name: 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](#).

- **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

DEV-AWINGU ▾
Configure ▾
Manage ▾
Changes
Global ▾

API Token Based Authentication

Whitelisted Subnets

Whitelisted Subnets

☒ Enabled
 ☐ Disabled

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

Cancel Apply

System Settings - © 2012-2018 Awingu N.V. - [Eula](#)
4.1

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**:

Awingu.com

Workspace

Files

Applications

Manage API token

Close x

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.

English United States

Preferred language

Please enter your password to generate or disable a token:

Password

Generated token for dev-awingu\kerwyny:

Save

Generate new token

Disable token

kerwyny

Licensed to Awingu
Awingu 4.1 © 2012 - 2018

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

Reverse Proxy

DEV-AWINGU

Configure

Manage

Changes

Global

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.

Cancel

Apply

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.

Skype for Business Online Integration

See Microsoft Skype for Business Online.

SSO Identity Provider (IdP)

DEV-AWINGU
Configure
Manage
Global

SSO Identity Provider (IdP)

State

Disabled

Issuer

/

Logout URL

/

Certificate

Private Key

SSO Services

Name	State
✓ Azure AD / Office 365	✗
✓ Confluence	✗
✓ Dropbox	✗
✓ Freshdesk	✗
✓ Google Apps	✗
✓ JIRA	✗
✓ Okta	✗
✓ Salesforce	✗
✓ Zoho	✗

Items per page
10

1 / 1

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

Awingu allows SSO (Single Sign-On) integration with SaaS services. In case SSO is enabled, Awingu serves as Identity Provider (IdP), as defined in SAML V2.0. This allows you to:

- Sign-in automatically to SaaS services when accessed via Awingu
- Use your account on Awingu to sign-in on SaaS services

This section contains the settings required for all SaaS services, while the next session [SSO Services](#) handles the settings per service.

- **State:** Enable or Disable IdP functionality in Awingu for all SaaS services.
- **Issuer:** URL from which Awingu is reachable for the end-users, e.g. <https://awingu.mycompany.com/>.
- **Logout URL:** The logout URL redirects the browser to this URL, once the user logs out of the SaaS application that is configured for SSO. By default, the Logout URL is '/' (i.e goes to Awingu main page), but it can hold any valid URL.

SAML V2.0 mandates that responses are cryptographically signed. Awingu uses a certificate and private key to generate the SAML responses. The SaaS service validates the response with the certificate, which should be configured in the service. As there is no certificate authority involved, the certificate can be self signed. Note that the certificate-key pair is the same for all configured SaaS services configured within one Awingu domain.

- **Certificate:** The public X.509 certificate for the provided Issuer in **.crt format/.pem format**, ASCII file, starting with:
-----BEGIN CERTIFICATE-----
- **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-----

The way you generate keys and certificates often depends on your development platform and programming language preference. Here an example is shown how to generate a certificate using [openssl](#) (download for Windows [here](#)) via the command line:

```
set OPENSSL_CONF=C:/OpenSSL-Win32/bin/openssl.cfg
C:\OpenSSL-Win32\bin\openssl.exe genrsa -out private_key.pem 2048
C:\OpenSSL-Win32\bin\openssl.exe req -new -x509 -days 3650 -key
private_key.pem -out certificate.pem
```

When the "Common Name" is asked, please enter your domain name, e.g. [mycompany.com](#).

An alternative way to generate keys: https://www.samltool.com/self_signed_certs.php (note: generating keys via a third party always induces a security risk).

Security Warning

The private key should be kept secret at all times. If this key gets compromised, unauthorized individuals can access to your corporate accounts of the SaaS services.

SSO Services

Awingu supports several SaaS services for Single Sign-On (SSO) out of the box. In this section, you can enable and configure each service. Please refer to [Single Sign-On for SaaS Applications](#) for step-by-step guidance.

- [Azure AD / Office 365](#)
- [Google Apps](#)
- [Okta](#)
- [Salesforce](#)

To support other SaaS services than the ones supported by Awingu, you can use Okta or Azure AD as **IdP Proxy**, which can redirect those services to Awingu. For more information, please refer to:

- [Use Okta as IdP Proxy](#)
- [Use Azure AD as IdP Proxy](#)

Application Sessions

The screenshot shows the 'Application Sessions' configuration page in the Awingu interface. At the top, there is a navigation bar with 'DEV-AWINGU', 'Configure', 'Manage', 'Changes', and 'Global'. The main content area has a title 'Application Sessions' and two configuration sections. The first section, 'Recordings Upload', has a radio button set to 'Enabled' and a text input field for 'Recordings Upload URL'. Below the URL field, a red error message states 'Required, supported protocols: http and smb'. The second section, 'Keepalive Disconnected Timeout', has a text input field with the value '15' and a label 'Timeout in minutes'. Both sections have 'Cancel' and 'Apply' buttons. At the bottom, a footer bar contains 'System Settings - © 2012-2018 Awingu N.V. - Eula' and the version number '4.1'.

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 in user groups with the *record* label (cf. [User Connector Configuration](#))

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 that only authorized personnel can access the server defined in Recordings Upload URL!

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).

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
- Adding applications manually
- Importing applications with a CSV file
 - Generating a CSV file
 - Importing a CSV file
- Configuring shortcut keys

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 2 flavors:
 - **RDP**: will make use of the regular Remote Desktop Protocol. Full desktops can only be provided via this protocol.
 - **RemoteApp**: 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 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.

The technical flow of opening a streamed application (RDP or RemoteApp), is documented [here](#).

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

- **Web Applications**. 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).
 - Without reverse proxy: The browser will be redirected directly to the URL of the web application, which needs to be reachable from the end-user's device.
 - With reverse proxy:
 - 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.

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 available to do so.

Adding applications manually

Click on **Add** to define a new application and scroll down.

The screenshot shows the top navigation bar of the Awingu interface with tabs for 'DEV-AWINGU', 'Configure', 'Manage', 'Changes', and 'Global'. Below the navigation bar, there is a section titled 'Add Application'. This section contains a form with a label 'Name' and an adjacent text input field. A vertical scrollbar is visible on the right side of the form area.

Required

Description

Icon



Choose File

No file chosen

Protocol

Required

Command

Unicode Keyboard
Support

☒ Enabled

☐ Disabled

Working Folder

Only available for RDP Applications

Categories

Available items

- Office
- RDP App 2008 Çæßøý #"/@&
- RDP App 2012 Çæßøý #"/@&
- RDP App 2016 Çæßøý #"/@&
- RemoteApp 2008 Çæßøý #"/@&
- RemoteApp 2012 Çæßøý #"/@&
- RemoteApp 2016 Çæßøý #"/@&
- Selenium
- Servers
- Smartcard Çæßøý #"/@&%*
- System

Select all

Chosen items

Select all

Media Types

Available items

- application/acrobat
- application/msword
- application/pdf
- application/rtf
- application/txt
- application/vnd.ms-excel
- application/vnd.ms-excel.addi
- application/vnd.ms-excel.shee
- application/vnd.ms-excel.shee
- application/vnd.ms-excel.tem
- application/vnd.ms-powerpoin

Chosen items

Select all

Select all

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.

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>".

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.

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.

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.

Cancel

Add

The following settings can be configured:

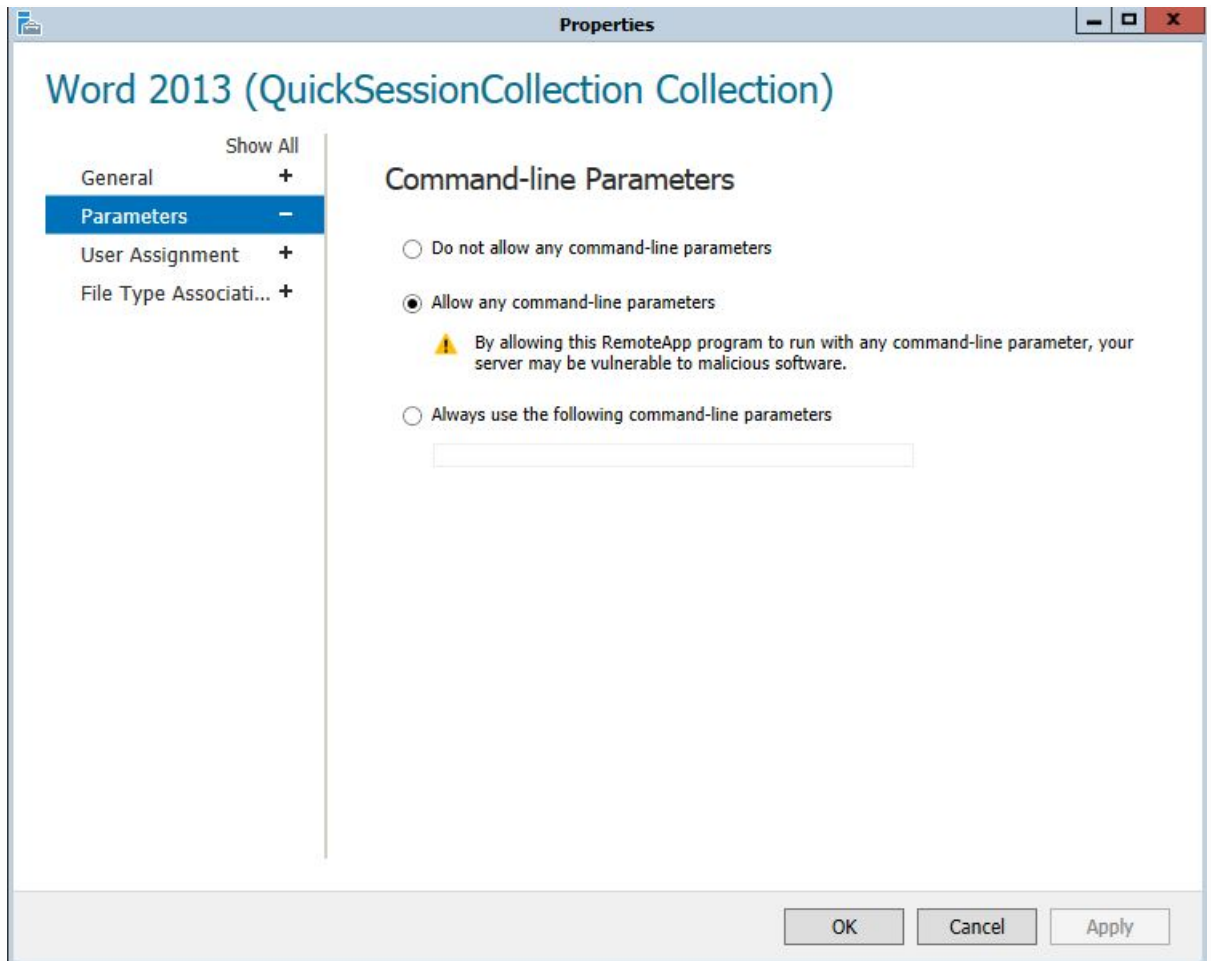
- **Name:** The application name as it will appear in the Awingu user interface.
- **Description:** description of the application, not visible to end-users.
- **Icon:** The application icon that will be visible to the end-user in the Awingu user interface. When you upload an icon, it is saved to the database and automatically propagated to all Awingu front-end instances in your Awingu deployment. Only ICO, JPG and PNG are allowed.
- **Protocol:** possible options:
 - **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 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.
 - **Web Application** is not served through the RDP gateway component. Instead, when launching a Web application, a separate tab will be opened. You can specify whether to use the built-in reverse proxy for HTTP(S).

When both Remote Applications and RDP Applications are supported on your application server, we strongly recommend to use Remote Application.

- **Alias / Command / Destination URL** (depending on the chosen protocol):
 - For Remote Applications, provide the Remote Application alias.
 - For RDP Applications, the command is the full path to the program executable. If left empty, a full desktop will be launched.
 - For Web Applications, you can provide the URL the application can be accessed.
 - When not using the built-in reverse proxy, that URL needs to be accessible for the end-user.
 - When using the built-in reverse proxy, that URL needs to be accessible for Awingu.
- **Reverse Proxy** (*Only available for Web Applications*): Enable or disable the use of the built-in reverse HTTP(S) proxy of Awingu for this application.
- **Source Host Header** (*Only available for Reverse Proxied Web Applications*): 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).
- **Destination Host Header** (*Only available for Reverse Proxied Web Applications*): 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** (*Only available for Reverse Proxied Web Applications*): 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 probably might disable this feature.
- **Single Sign-On** (*Only available for Reverse Proxied Web Applications*): 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.
- **Domain For Single Sign-On** (*Only available for Reverse Proxied Web Applications with Single Sign-On enabled*): If enabled the domain name (NETBIOS\username) will be included in the HTTP authorization header that is passed to the Web application.
- **Unicode Keyboard Support** (*Only available for RDP/Remote Applications*): 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.
- **Working Folder** (*Only available for RDP Applications*): Folder into which an application needs to be launched, i.e. the current working directory. This can remain empty.
- **Categories:** Associate zero, one or more application [categories](#) to this application.
- **Media Types** (*Only relevant for RDP/Remote Applications*): Associate zero, one or multiple media types with this application for viewing or editing.

If you want to associate media 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.



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

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

- **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 activate [session recording](#) for this application for all users (needs to be enabled).
- **Server Labels** (*Only relevant for RDP/Remote Applications*): 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.
- **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.
- **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.
- **Start in Foreground** (*Only available for RDP/Remote Applications*): 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** (*Only available for RDP/Remote Applications*): 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** (*Only available for RDP/Remote Applications*): 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** (*Only available for RDP/Remote Applications*): 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 be shown to the user, too.

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:

- Unicode Keyboard Support
- Categories
- Media Types
- Labels
- Server Labels
- User Labels
- Auto Start Labels
- Notifications

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

Configuring shortcut keys

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

Click on the Shortcut Keys 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 keyboard 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

Application Server Management

- [Introduction](#)
- [Adding/Configuring Application Servers](#)
 - [Importing applications servers](#)
 - [Manually adding/editing application servers](#)
- [Further Configuration of the Applications](#)
- [Remote Desktop Service Connection Broker](#)

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 [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 applications 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.

Import

1. Select Servers

Start typing to search

✓ Name ▲	Host Name	Dn
✓ AD2012	AD2012.stack.awingu.com	CN=AD2012,OU=Domain Controllers,DC=...
✓ AD2012-2	AD2012-2.stack.awingu.com	CN=AD2012-2,CN=Computers,DC=stack,...
✓ APP1	APP1.stack.awingu.com	CN=APP1,OU=SGO-APPservers,DC=stac...
✓ APP2	APP2.stack.awingu.com	CN=APP2,OU=SGO-APPservers,DC=stac...
✓ APP2008	APP2008.stack.awingu.com	CN=APP2008,OU=SGO-APPservers,DC=...
✓ APP2012	APP2012.stack.awingu.com	CN=APP2012,OU=SGO-APPservers,DC=...
✓ APP3	APP3.stack.awingu.com	CN=APP3,OU=SGO-APPservers,DC=stac...
✓ APP4	APP4.stack.awingu.com	CN=APP4,OU=SGO-APPservers,DC=stac...
✓ APP5	APP5.stack.awingu.com	CN=APP5,OU=SGO-APPservers,DC=stac...
✓ APP6	APP6.stack.awingu.com	CN=APP6,OU=SGO-APPservers,DC=stac...

Items per page 10 ▾

2. Set Default Settings

Port 3389

Max Connections

Required

State ☐ Enabled☐ Disabled

Required

Labels

Cancel

Import

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).
- **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.
- **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.
- **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.

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.

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](#)
- [Supported protocols](#)
- [Adding/editing drives](#)

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:
 - SMB 3.0 for Windows Server 2008 R2, 2012, 2012 R2 and 2016
 - Samba3 server.
- WebDAV with support for:
 - IIS for Windows Server 2008 R2, 2012, 2012 R2 and 2016 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).

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.

STACK
Configure
Manage
Global
Apply Changes

Add Drive

Name
Required

Description

Backend
Required

URL
Required

UNC

Domain Use
☐ Enabled
☐ Disabled

Labels

User Labels

Cancel
Add

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

- **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
If access to DFS namespaces is required or when UDP broadcast is blocked (e.g. on Public Clouds), please make sure to enable the Use SMB/CIFS via port 445 (Direct TCP) feature [Connectivity Settings](#).
 - WebDAV
 - Microsoft OneDrive For Business. Mored 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
- **Awingu 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:** 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.
- **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 users 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](#).

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.

The screenshot shows the 'Add File Type' dialog box within the Awingu System Settings application. The interface has a dark header bar with navigation tabs: 'DEV-AWINGU', 'Configure', 'Manage' (selected), and 'Changes'. A 'Global' dropdown is on the right. The dialog itself has a title bar 'Add File Type' and contains the following fields and controls:

- File Extension:** A text input field with a red border and the label 'Required' below it.
- Description:** A larger text input field.
- Icon:** A section with a question mark icon, a 'Browse...' button, and the text 'No file selected.'
- Apps:** A section with two columns: 'Available items' and 'Chosen items'. Each column has a search input field labeled 'Start typing to search'. Below the search fields, the 'Available items' list includes: 'API Docs', 'Dashboard', 'Advanced Insights', 'Preview', 'Recorded Session Player', 'System Settings', 'Bob50 (app2012) Çæβøý #"/ç', 'Microsoft Word (app2008) Çæ', 'Microsoft Word RDP (app2008', and 'Microsoft Word RDP (app2012'. There are right and left arrow buttons between the two lists. At the bottom of each list is a 'Select all' button.
- Buttons:** 'Cancel' and 'Add' buttons are at the bottom right of the dialog.

The footer of the application window displays 'System Settings - © 2012-2018 Awingu N.V. - Eula' and the version '4.1.1'.

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](#)
- [User Labels](#)
 - [Importing Labels](#)
 - [Example of Use of User Label](#)
- [Server labels](#)
- [Labels](#)

Introduction

Labels allow you to group users, applications, drives and servers by different properties.

These groupings can not only be used to easily filter items in lists or reports, but also to link different items with each other.

Labels are used to authorize end-users to applications, drives and features in an automated and scalable way.

When an end-user logs in to Awingu, the credentials are passed to a User Connector that authenticates the user with an external authentication service, i.e. a Microsoft Domain Controller or an LDAP server.

See the details of the [Sign-in Process](#).

Each time a user signs-in, the labels will be defined for that user. Whether the users has the labels *admin*., *staff* or *record*., can be defined in [User Connector Configuration](#). All other labels can be defined here, in System Settings.


Labels are defined by a key and a value. There are 3 types of usage of labels:

- User labels
- Server labels
- Labels

In case there is no confusing, the general term "label" is used in System Settings.

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.

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 <i>group</i> key needs to be made. You can use <i>Import groups from AD</i> 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 <i>username</i> key needs to be made. You can use <i>Import users from AD</i> 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 <i>upn</i> 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 <i>ou</i> 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 <i>admin</i> in the User Connector Configuration .
staff	(empty)	Predefined user label. Do not remove. This label corresponds with the groups indicated as <i>staff</i> 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:

STACK
Configure
Manage
Global
Apply Changes

Labels

Start typing to search
Bulk Action

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

Items per page 10
1 / 1

Add Manually
Import groups from AD
Import users from AD

Import Group Labels

Select Groups

Start typing to search

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...

Items per page 10

1 / 7

Cancel Import

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:

Group	admin	record	staff
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	- Browser Check* - Microsoft Word - AutoCad - Cost Calculator - Euro Specs	- Home Drive - Engineering Drive - Managers Drive
Lucy: ou: Europe groups: Engineering	- Browser Check* - Microsoft Word - AutoCad - Cost Calculator - Euro Specs	- Home Drive - Engineering Drive
Maria: ou: Europe groups: Administrators	- Browser Check* - Dashboard* - System Settings* - Recorded Session Player* - Microsoft Word - Network Manager - Euro Specs	- Home Drive - Administrators Drive
Kim: ou: America groups: Accountancy, America Managers	- Browser Check* - Microsoft Word - Finance Explorer - Cost Calculator	- Home Drive - Accountancy Drive - Managers Drive
Patrick: ou: America Groups: HR, America Managers	- Browser Check* - 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.

User Management

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

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

All other parameters are read-only, and most of them 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](#). Administrators can change the user keyboard and locale settings in the configuration management console.

To logout users and close their application session, please refer to [Live Monitoring of Users Activity](#).

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.

STACK

Configure ▾

Manage ▾

Global ▾

Apply Changes

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. - Eula3.1.0

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](#).

DEV-AWINGU ▾

Configure ▾

Manage ▾

Changes

Global ▾

Changes

Filters

Action ▾

Resource type ▾

Resource id

User ▾

Authentication ▾

From

To

Reset

	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

10 items per page

1 / 29

Export CSV

System Settings - © 2012-2018 Awingu N.V. - [Eula](#) 4.1.1

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:

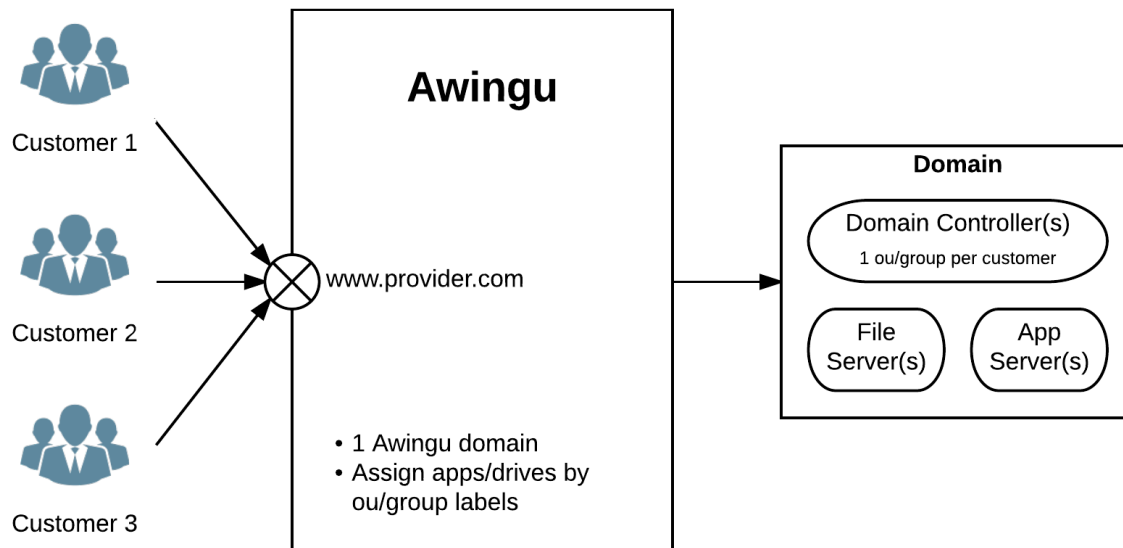
	Number of Awingu environments	Number of Awingu domains	Number of Windows domains	Branding per customer
1	One	One	One	✗
2	One	Multiple (one per customer)	One	✓
3	One	Multiple (one per customer)	Multiple (one per customer)	✓
4	Multiple (one per customer)	One per Awingu	One	✓
5	Multiple (one per customer)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

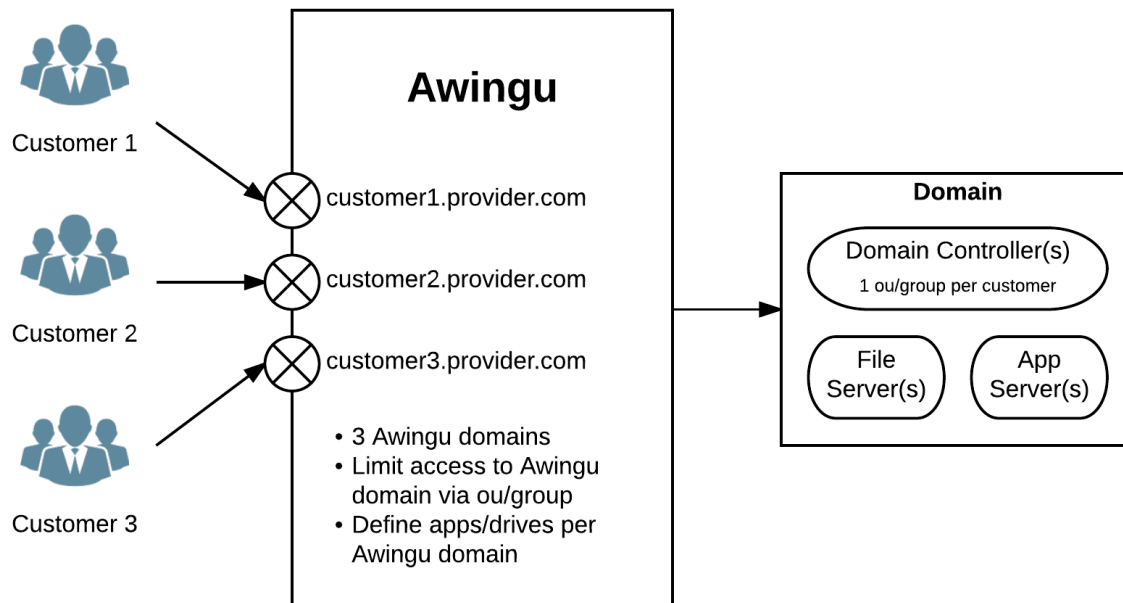
Configuration

- 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:

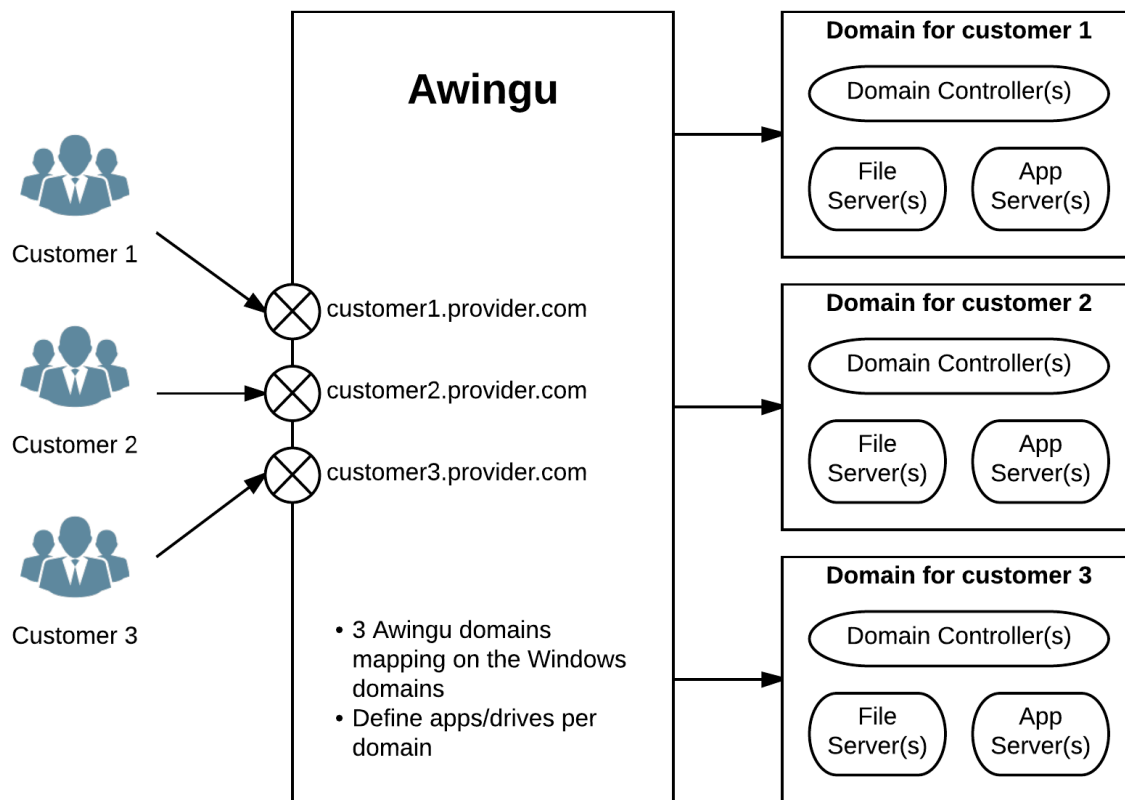
- Are the members of the Admin group defined for the domain for the service provider.
- Can manage all domains and global settings.

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:

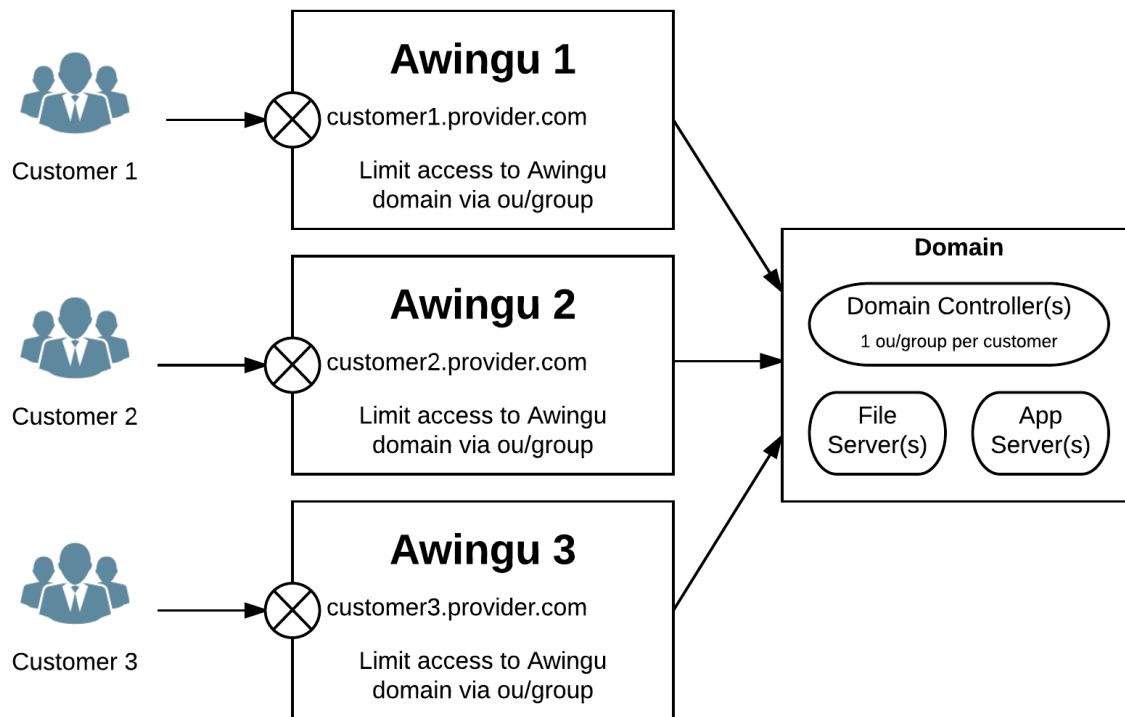
- Are the members of the Admin group defined for the domain for the service provider.
- Can manage all domains and global settings.

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 Awingu / 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.

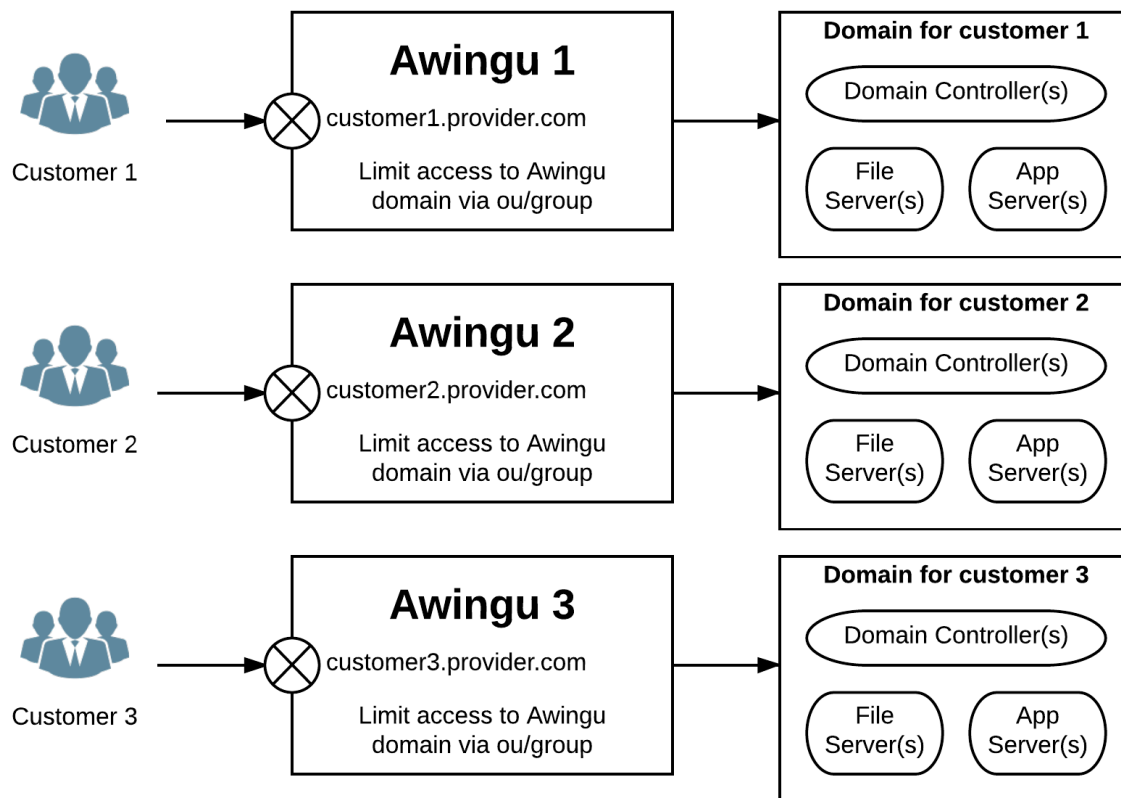
Configuration

- 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.

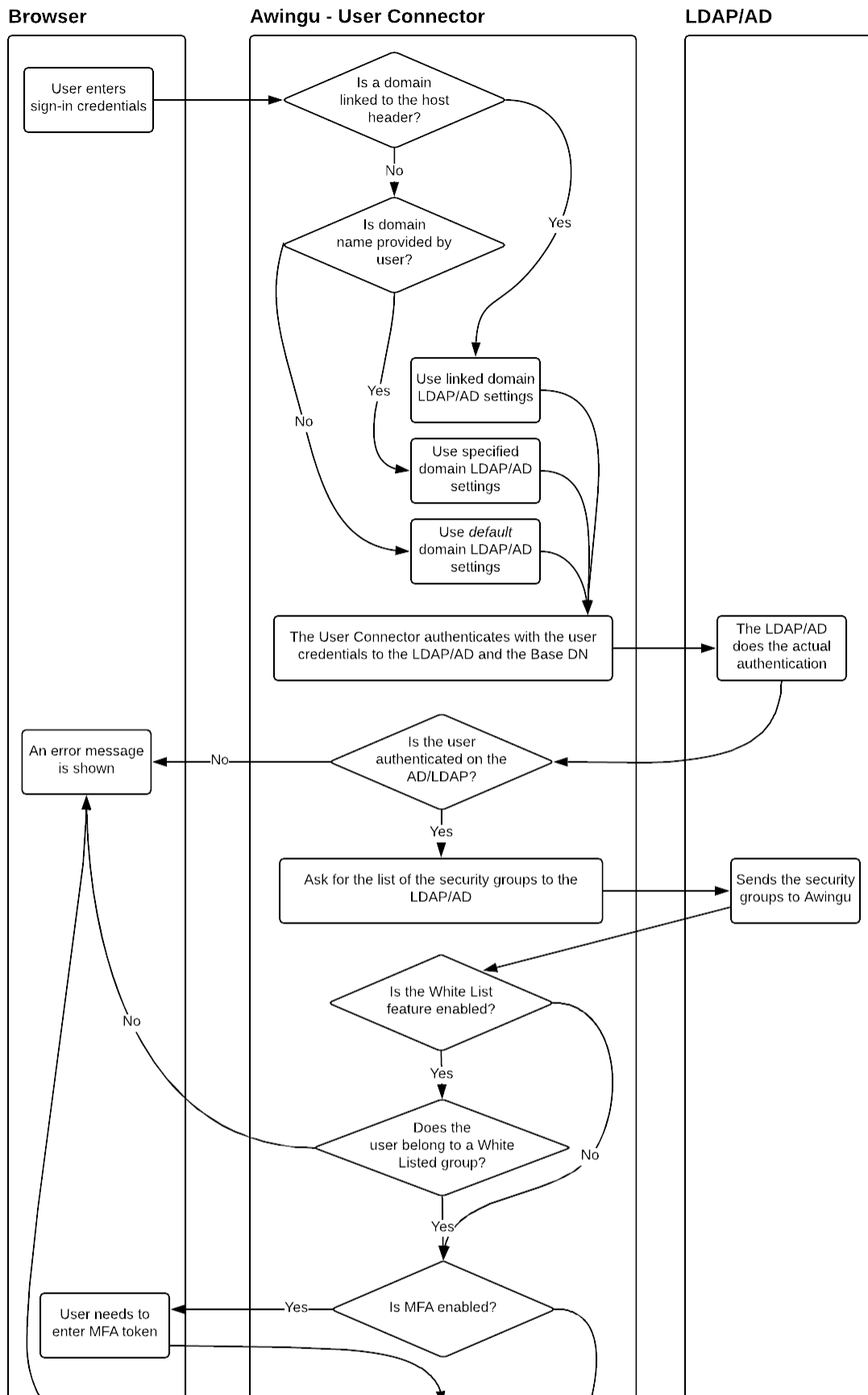
Administration

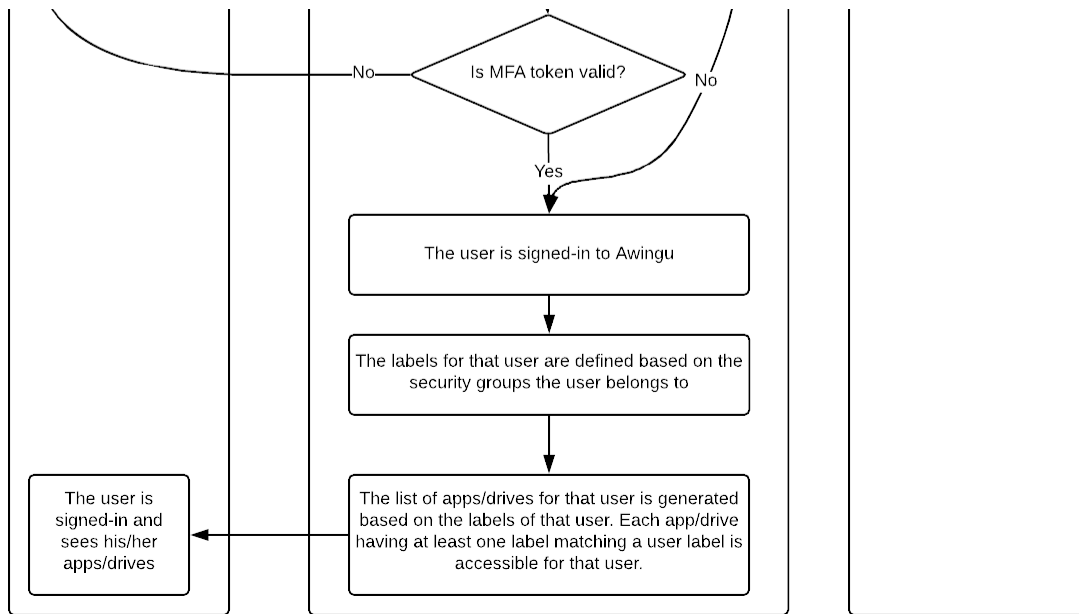
Each Awingu environment can be fully managed by the members of the Admin group defined for each environment.

How it works

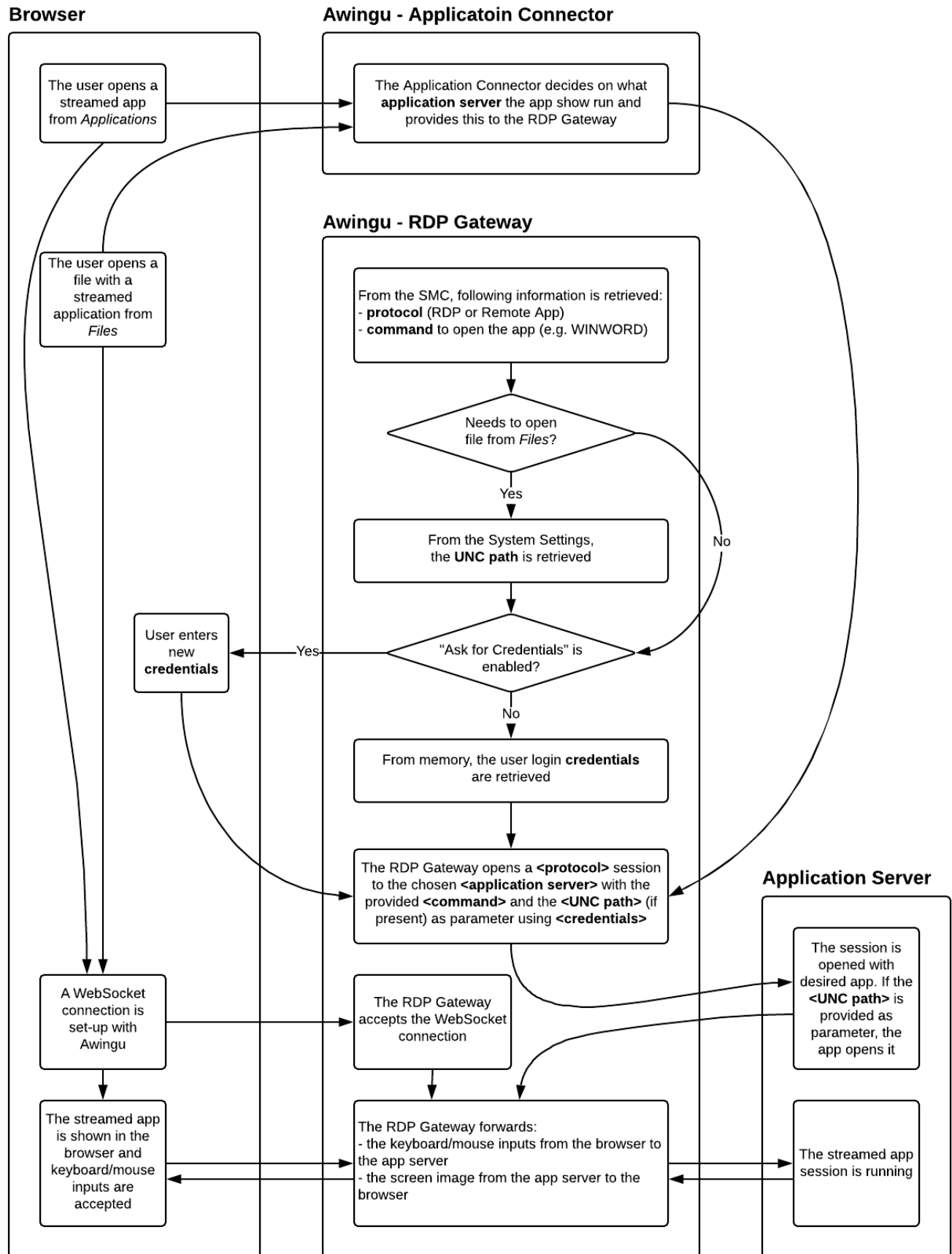
- [Sign-in Process](#)
- [Streamed Applications](#)
- [Reversed Proxied Web Applications](#)

Sign-in Process





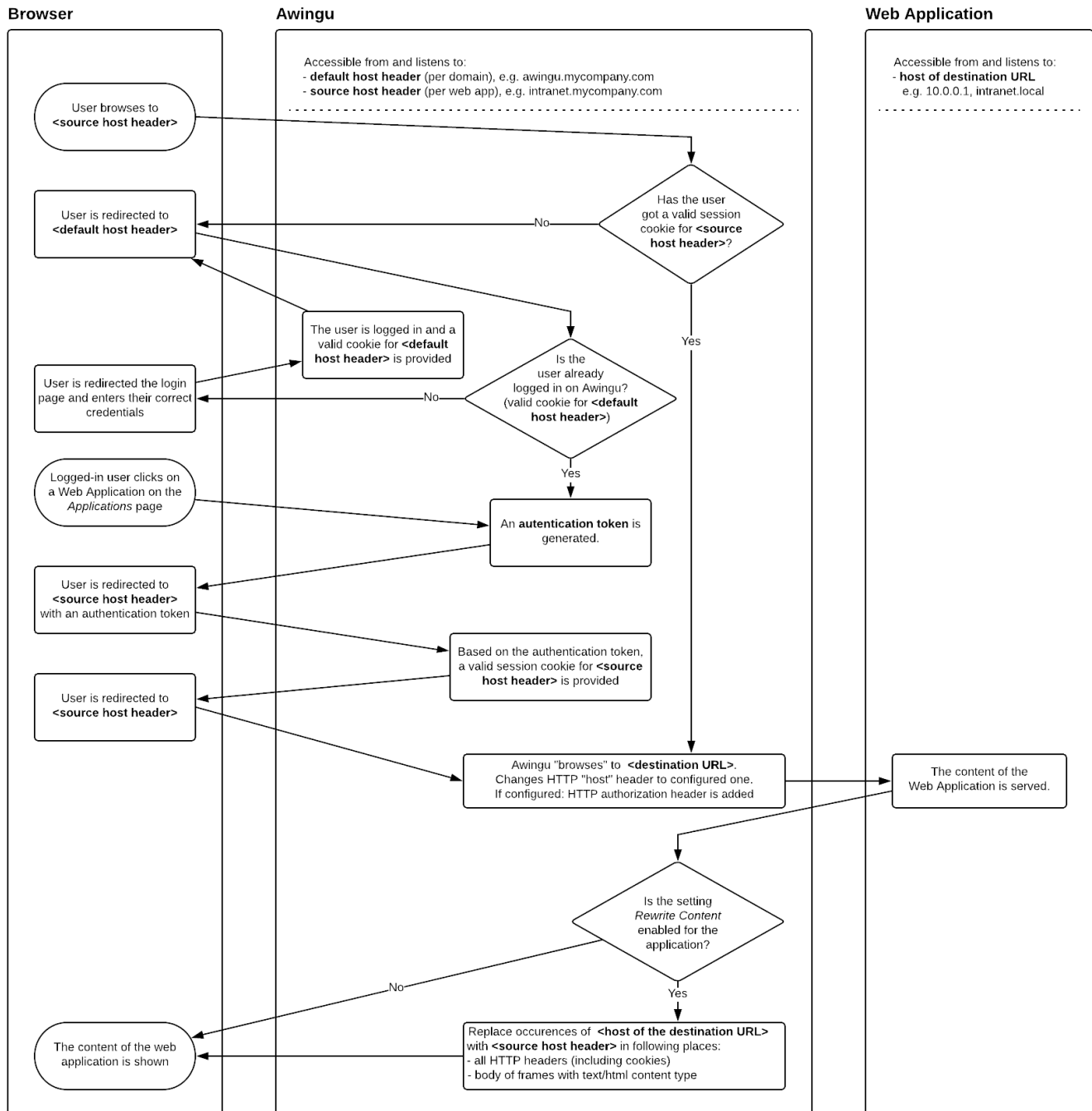
Streamed Applications



Reversed Proxied Web Applications

- Flow Chart
- HTTP Headers
 - Configuration 1: default
 - Configuration 2: smart web applications
 - Configuration 3: multiple smart websites on one web server

Flow Chart



HTTP Headers

This sections shows the HTTP Headers used in combination with the built-in reverse proxy.

This is the network example:

	Browser	Awingu	Web Server
IP address	172.22.2.162	172.16.4.69	172.16.0.62
Listening port	(none)	443	80
DNS entries	(none)	awingu.mycompany.com intranet.mycompany.com	intranet1.local*

* Use case 3 (cf. further)

We use following configuration example:

- Destination URL: `http://172.16.0.62:8000`
- Source Host Header: `https://intranet.mycompany.com`

#	Use case	Destination Host Header	Rewrite Content
1	The web server is not aware of any reverse proxy (default)	Same as Destination URL (default)	Enabled
2	The web server supports running behind a reverse proxy	Equals to Source Host Header	Disabled
3	The web server serves multiple sites (based on host headers) and supports running behind a reverse proxy	Same as Destination URL (default)	Disabled

In the example, the web application does following actions:

- Returning an HTML page
- Setting a cookie "locale=en"
- Setting a CORS header ([Cross-Origin Resource Sharing](#))

Configuration 1: default

Destination Host Header = host of Destination URL: this reflects in changing the header "Host" in the HTTP request.

Rewrite Content = Enabled: this reflects in the fact that all response headers (cookies and CORS) are modified.

As the web server is not aware of the presence of Awingu (meaning: it ignores the X-Forwarded header), it behaves as if Awingu would be the end-user.

HTTP Request	
Browser	Awingu
<div>Host: intranet.mycompany.com</div>	
Awingu	Web Server
<div>Host: 172.16.0.62:8000 X-Real-IP: 172.22.2.162 X-Forwarded-For: 172.22.2.162 X-Forwarded-Host: intranet.mycompany.com:443 X-Forwarded-Server: intranet.mycompany.com X-Forwarded-Port: 443 X-Forwarded-Proto: https</div>	

HTTP Response	
Web Server Awingu	
<pre> Content-Type: text/html Set-Cookie: locale=en; Domain=172.16.0.62; Path=/ Access-Control-Allow-Origin: 172.16.0.62 <html> <body> <h1>Hello World!</h1> My link </body> </html> </pre>	
Awingu Browser	
<pre> Content-Type: text/html Set-Cookie: locale=en; Domain=intranet.mycompany.com; Path=/ Access-Control-Allow-Origin: intranet.mycompany.com <html> <body> <h1>Hello World!</h1> My link </body> </html> </pre>	

Configuration 2: smart web applications

Destination Host Header = Source Host Header: this reflects in **not** changing the header "Host" in the HTTP request.

Rewrite Content = Disabled: this reflects in the fact that none of the response headers (cookies and CORS) are modified.

As the web server is aware of the presence of Awingu (it uses the X-Forwarded headers or it is configured like that), it will set the headers immediately correct for the end-user, so Awingu does not need to rewrite anything.

HTTP Request	
Browser Awingu	
<pre>Host: intranet.mycompany.com</pre>	
Awingu Web Server	

```
Host: intranet.mycompany.com
X-Real-IP: 172.22.2.162
X-Forwarded-For: 172.22.2.162
X-Forwarded-Host: intranet.mycompany.com:443
X-Forwarded-Server: intranet.mycompany.com
X-Forwarded-Port: 443
X-Forwarded-Proto: https
```

HTTP Response

Web Server Awingu

```
Content-Type: text/html
Set-Cookie: locale=en; Domain=intranet.mycompany.com;
Path=/
Access-Control-Allow-Origin: intranet.mycompany.com

<html>
  <body>
    <h1>Hello World!</h1>
    <a href="https://intranet.mycompany.com/mylink.html">My link</a>
  </body>
</html>
```

Awingu Browser

```
Content-Type: text/html
Set-Cookie: locale=en; Domain=intranet.mycompany.com;
Path=/
Access-Control-Allow-Origin: intranet.mycompany.com

<html>
  <body>
    <h1>Hello World!</h1>
    <a href="https://intranet.mycompany.com/mylink.html">My link</a>
  </body>
</html>
```

Configuration 3: multiple smart websites on one web server

Destination Host Header = host of Destination URL: this reflects in changing the header "Host" in the HTTP request.

Rewrite Content = Disabled: this reflects in the fact that none of the response headers (cookies and CORS) are modified.

The web server uses the Host header field to define which website to serve. The web server is however not configured to use the public DNS entries pointing to Awingu.

As the web server is aware of the presence of Awingu (it uses the X-Forwarded headers), it will set the headers immediately correct for the end-user, so Awingu does not need to rewrite anything.

HTTP Request	
Browser Awingu	
<div>Host: intranet.mycompany.com</div>	
Awingu Web Server	
<div>Host: intranet1.local X-Real-IP: 172.22.2.162 X-Forwarded-For: 172.22.2.162 X-Forwarded-Host: intranet.mycompany.com:443 X-Forwarded-Server: intranet.mycompany.com X-Forwarded-Port: 443 X-Forwarded-Proto: https</div>	

HTTP Response	
Web Server Awingu	
<div>Content-Type: text/html Set-Cookie: locale=en; Domain=intranet.mycompany.com; Path=/ Access-Control-Allow-Origin: intranet.mycompany.com <html> <body> <h1>This is Intranet 1</h1> My link </body> </html></div>	
Awingu Browser	

```
Content-Type:          text/html
Set-Cookie:            locale=en; Domain=intranet.mycompany.com;
Path=/
Access-Control-Allow-Origin: intranet.mycompany.com
```

```
<html>
  <body>
    <h1>This is Intranet 1</h1>
    <a href="https://intranet.mycompany.com/mylink.html">My link</a>
  </body>
</html>
```

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](#)
- [Monitoring Servers and Components](#)
- [Awingu License Tracking](#)
- [Live Monitoring of Users Activity](#)
- [Monitoring the Application Connector](#)
- [Insights Reporting](#)
- [Audit Reporting](#)
- [Anomaly Reporting](#)

Status Overview of Services on All Servers

The **Status** tab of the Dashboard provides a heatmap 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. Three 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. It shows the number of named users for the past 12 months as well as for the current month. It counts the number of named users that are known in the Awingu database over the course of a calendar month. Named users that are in the database and that have not been explicitly removed before the end of the previous calendar month will be counted, even when these users do not log in to Awingu in the current calendar month. The current calendar month value tracks the number of named users up-to the current date.

For users that have been removed from the database, an entry will be re-created at next login time.

Note that the values are not updated real-time, but twice a day.

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. One user simultaneously signed-in to Awingu from two different devices/browsers counts as two user sessions.

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 and terminate 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.

If users are simultaneously connected from multiple browsers, e.g. connecting simultaneously from multiple devices, these will be counted as multiple concurrent user sessions.

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:

- The table is sorted according to the number of user sessions per user.
- 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 (eye icon).
- 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.
- Each application session can be disconnected (still visible in the side bar of the user) and terminated (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.

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

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
Labels	All (user) labels fetched from the AD/LDAP
Location	Coordinates/ based on geo IP (which is indicative).

Note that first the longitude and then the latitude is shown!

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

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 chunks 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	Description
COUNTRY_MISMATCH	Same user is logged in in 2 different countries simultaneously
TRAVEL_SPEED	The distance between to logins is too far to travel at realistic speed
TOO_MANY_FAILED_ATTEMPTS	A user uses the wrong password more than 3 times
NEW_BROWSER	A user logs in with a new browser

For each detected anomaly, following information is provided:

Property	Meaning
Timestamp	Timestamp of the detected anomaly
Domain	Domain of the user
Category	Only LOGIN category is 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
- Using Awingu on existing Citrix infrastructure
- SSL offloader, reverse proxy or loadbalancer settings
- Multi Factor Authentication
- Single Sign-On for SaaS Applications
- Microsoft OneDrive for Business
- Microsoft Skype for Business Online
- Smart Card Redirection
- Automate Awingu via the REST API

Integrating with existing Windows environment

- Introduction
- Using the Active Directory Server as NTP server
- Organizational Units for users and application servers
- Group Policy recommendations
 - GPOs for the Awingu users
 - GPOs for the applications servers
- Set-up Drives connectivity
 - CIFS connectivity:
 - WebDAV drives:
 - To set-up WebDAV via IIS (version 8)
 - WebDAV support for large files
 - WebDAV adding MIME Type
 - WebDAV create default MIME type
- Set-up the Application Servers
 - Supported Windows versions
 - Enabling audio support
 - RDP vs RemoteApp
 - Windows 2008 R2 Application server
 - Install Remote Desktop Services
 - Configuration
 - Configure RemoteApp Setting
 - Add/Remove RemoteApp programs
 - Additional Remarks
 - Windows 2012 (R2) and 2016 Application server
 - Install Remote Desktop Services
 - Configuration
 - Configure deployment service
 - Configure RemoteApp Collections
 - Configure RemoteApps
- Using Windows AD Administrative Center

Introduction

Although there are many possibilities to the Awingu platform 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](https://www.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
```

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 applications 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**.
 -  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:
 -  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).

For Windows 2012 R2 and 2016 (after update KB3161949 has been applied), you need to enable Direct TCP (in [Connectivity Settings](#)) if Awingu and the file server are in a different subnet.

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.

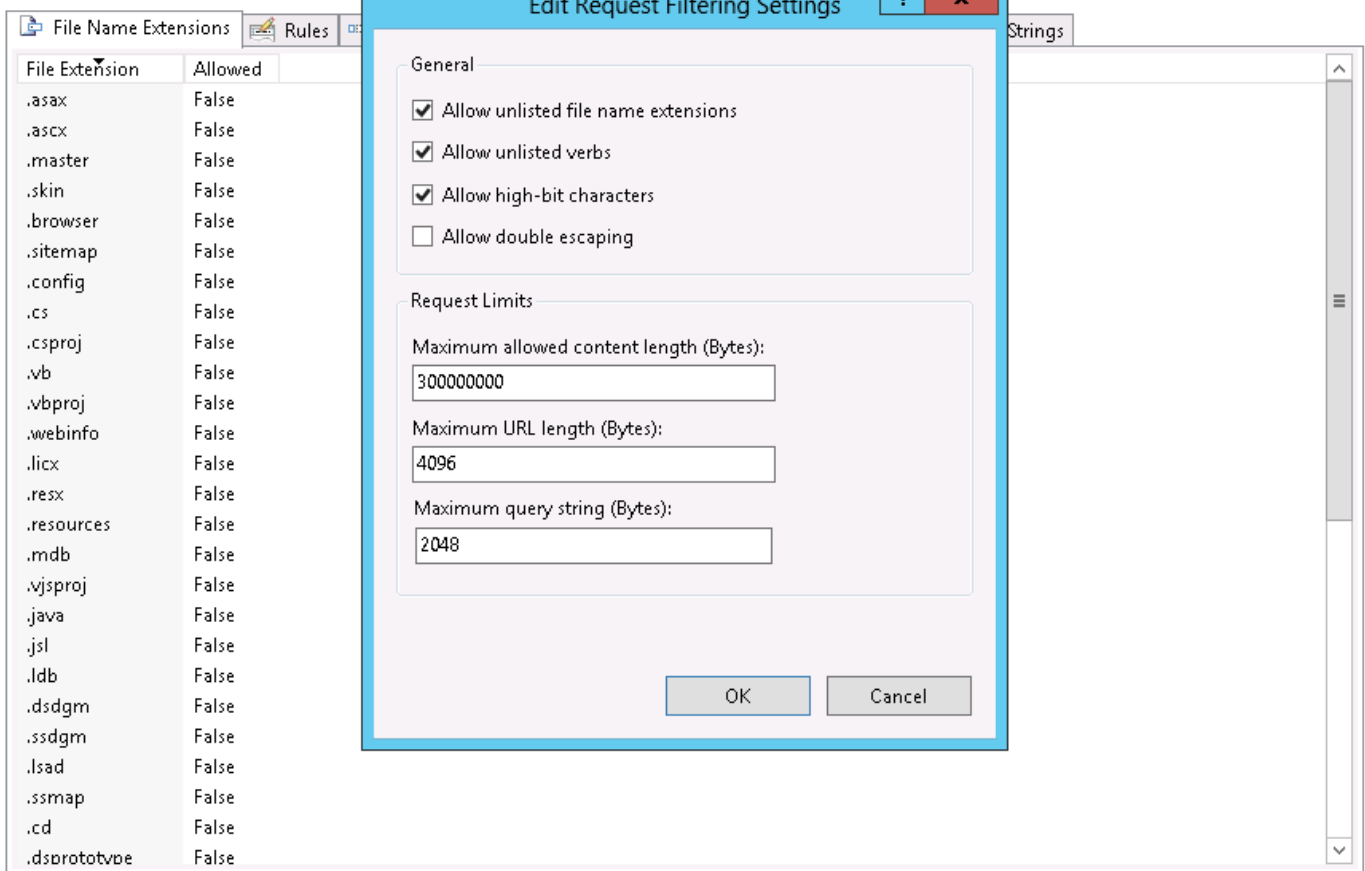
In summary

- Open the IIS Manager:
 - Click on the left pane to your WebDAV site.
 - Find and click 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.



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 (recommended)
- Windows 2016 (recommended)

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.

Note: when using certificates on the application servers, the ones Windows generates are not compatible with Awingu.

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 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

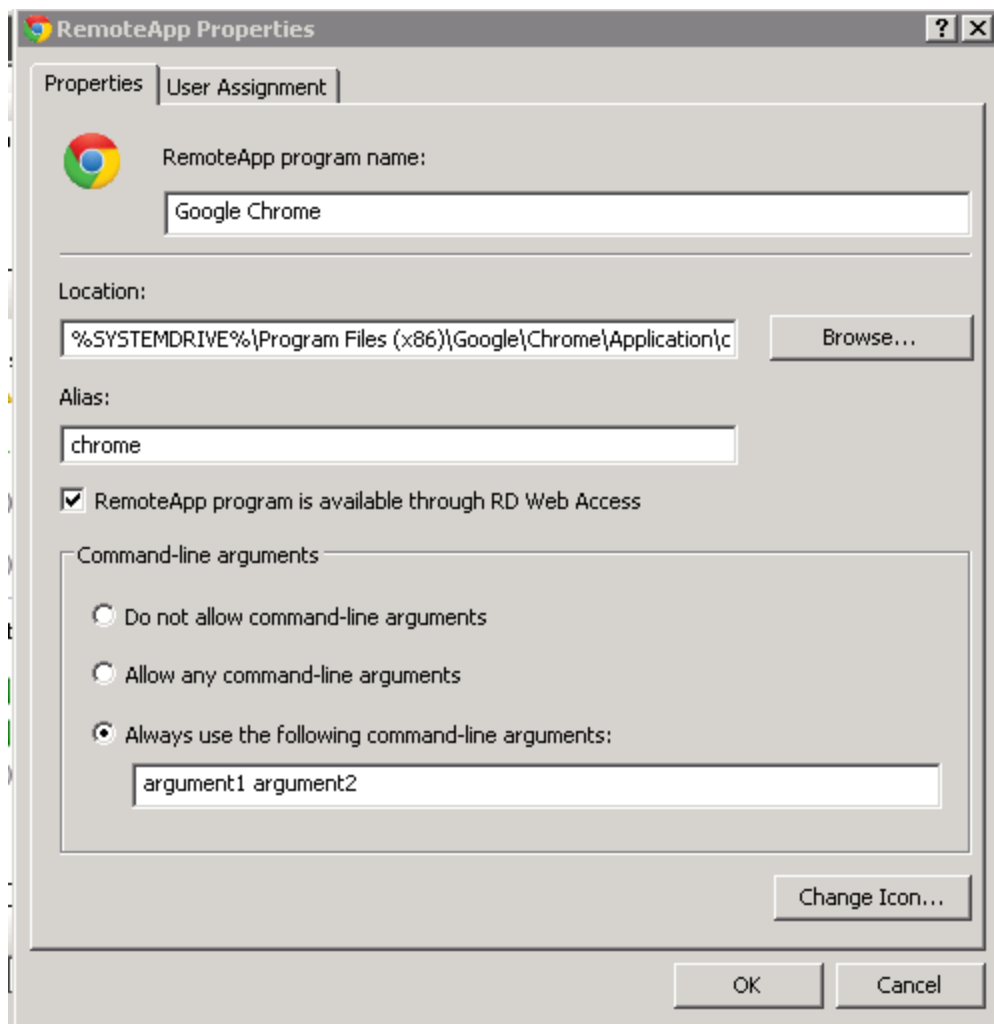
1. Open Server Manager. (click Start -> Administrative Tools -> Server Manager)
2. Under Roles, Remote Desktop Services, open RemoteApp Manager page, from the right menu select "Remote Session Host Server Setting".
3. Select "Do not allow users to start unlisted programs on initial connection", click 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:



Windows 2012 (R2) and 2016 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 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 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

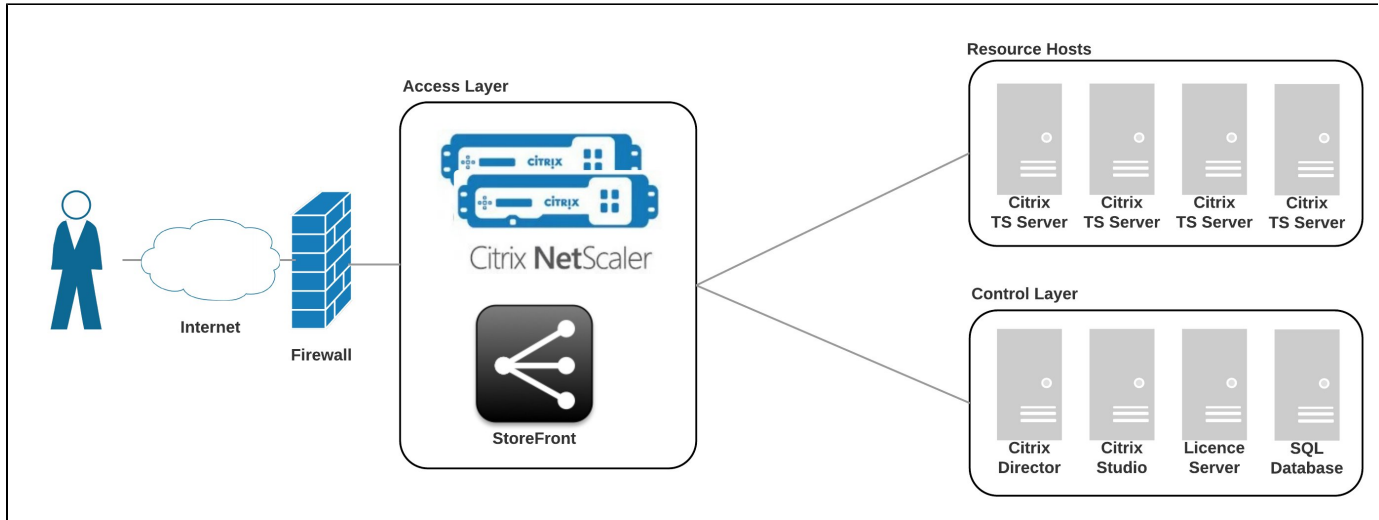
In Windows AD Administrative Center, the UPN is not required for a user. Awingu, however, requires this. Please provide a domain UPN as defined here: [https://technet.microsoft.com/en-us/library/cc772007\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc772007(v=ws.11).aspx)

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.

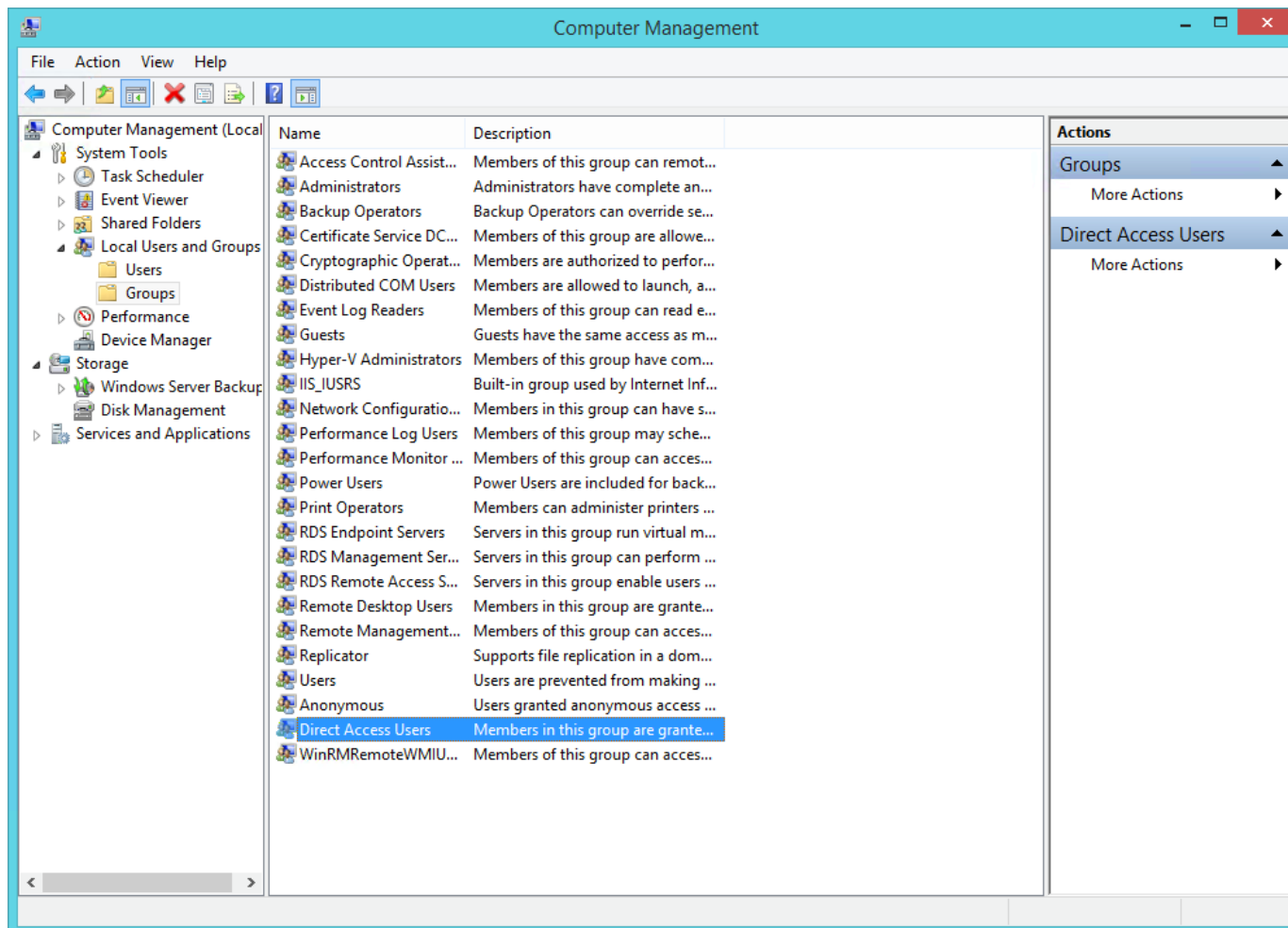
Note: as long Citrix is installed on the resource hosts, you need to have Citrix licenses for the RDP connections from Awingu to the resource hosts.

Preparation

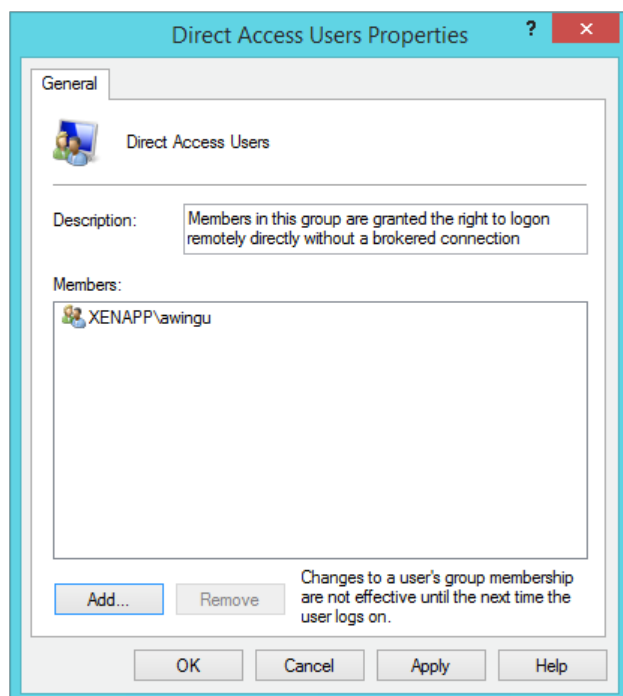
Download, install and configure Awingu as described in Admin Guide. The Citrix TS Servers (Resource Hosts) are the application servers to configure in [Application Server Management](#).

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:

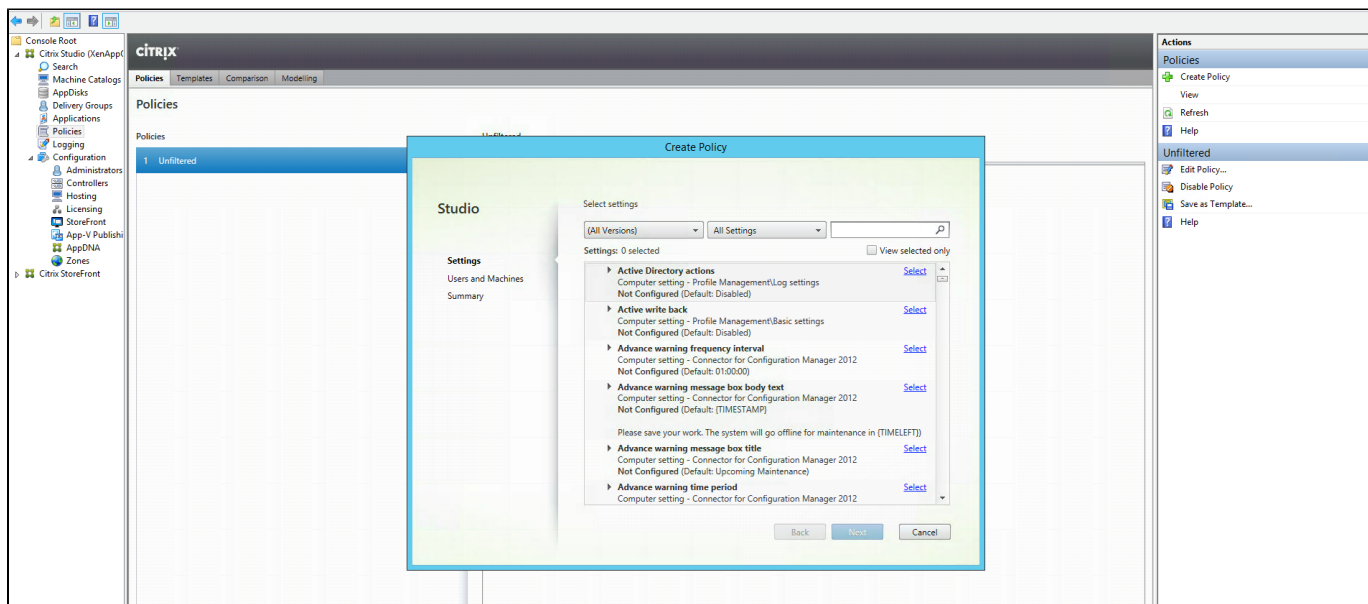


Add here the security group for the users which should have access:

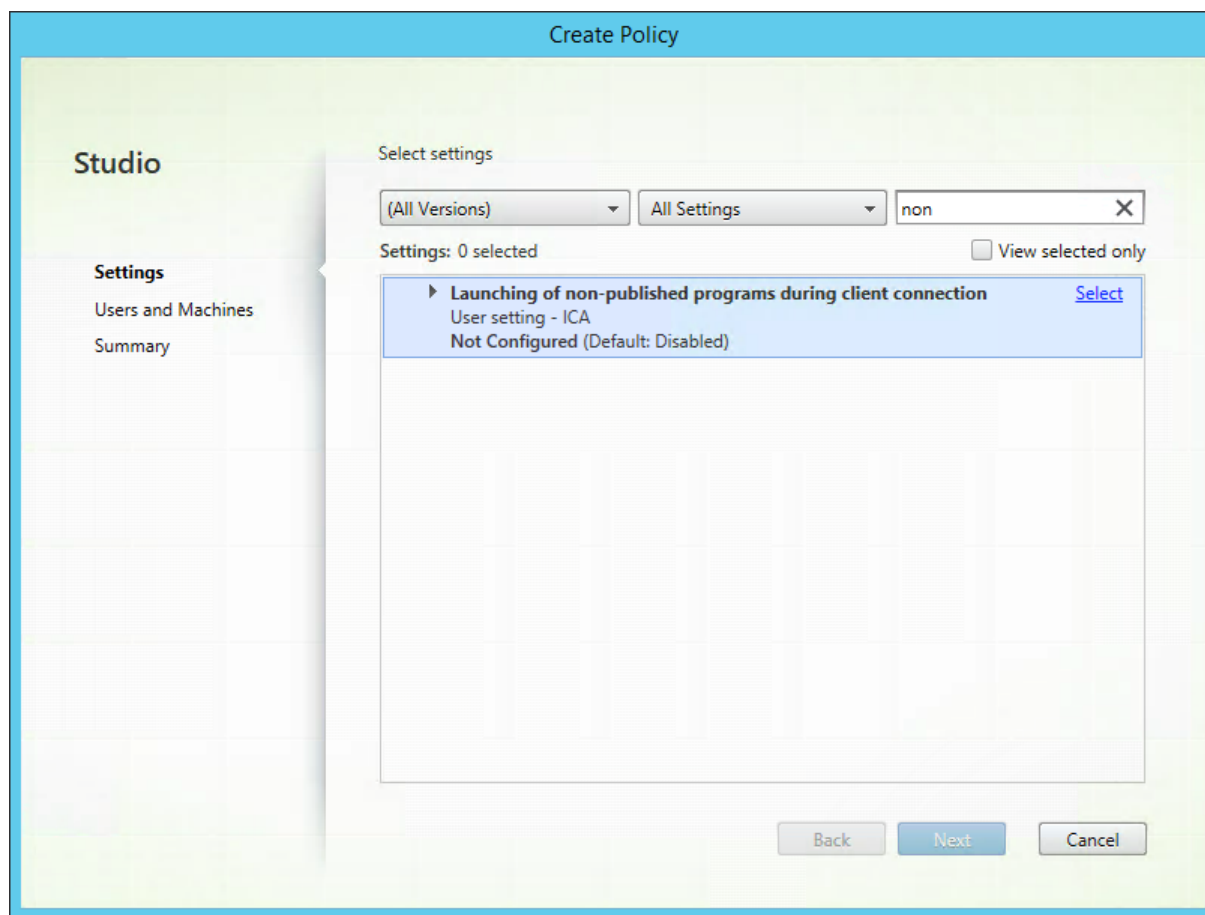


Enable RDP policy in Citrix studio

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:



In the search field search for: "Launching of non-published programs during client connection" and select it:



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

Studio

- ✓ Settings
- ✓ Users and Machines
- Summary**

Summary
View a summary of the settings you configured and provide a name for your new policy.

Policy name: ☒ Enable policy

Description:

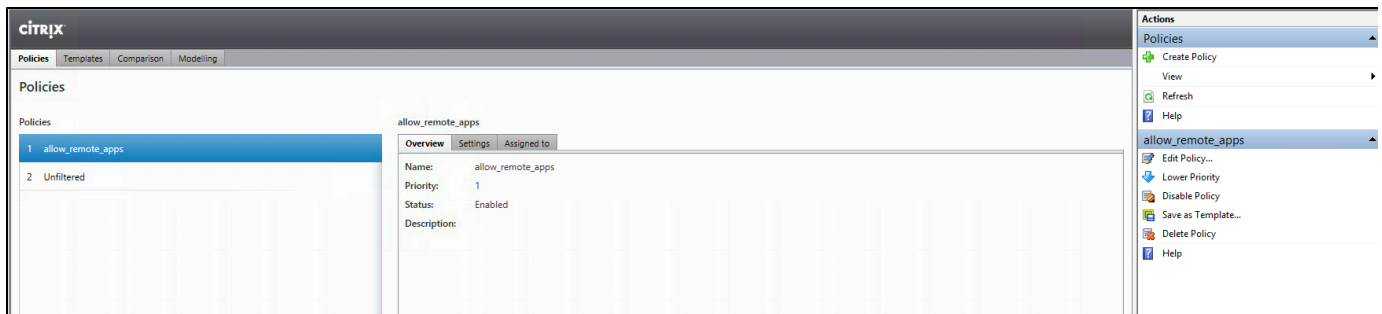
Settings configured: 1

Setting	Value
Launching of non-published programs	Enabled (Default: Disabled)

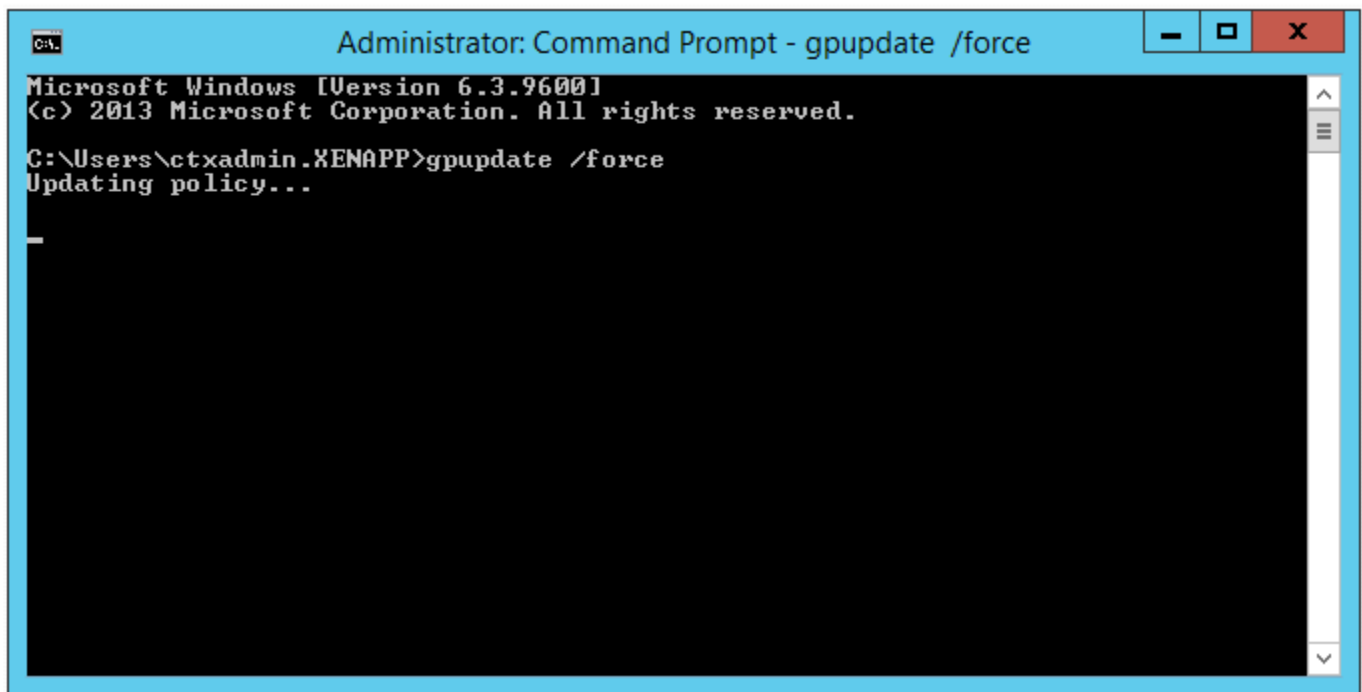
Assigned to: user and machine objects

The settings are applied to all objects in the site.

Set the policy priority higher:

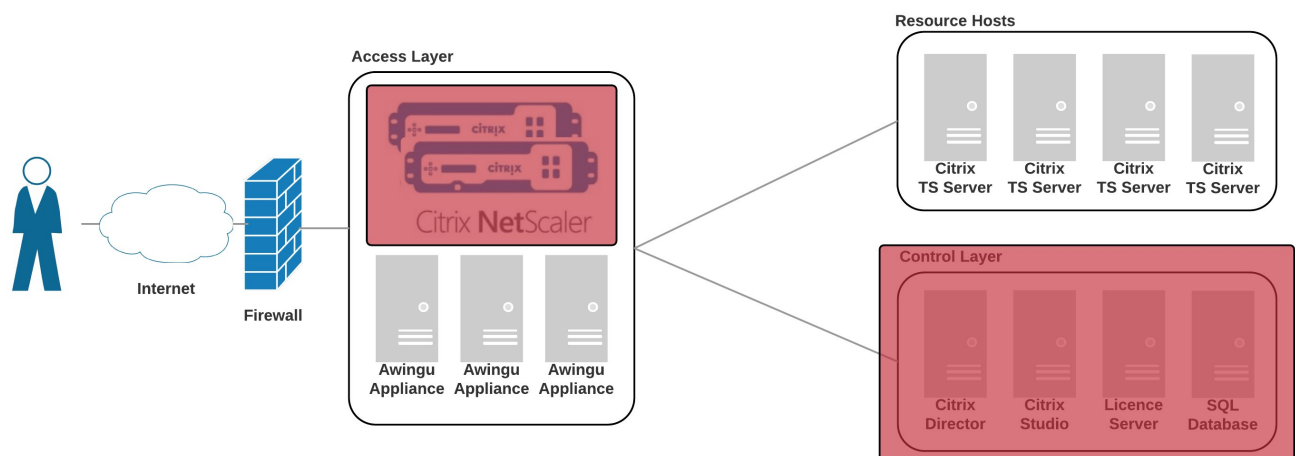


If you want to speed the policy up you can always update them manually:



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 allow 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 its 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 TLSv1.1 TLSv1.2;
    ssl_ciphers        'ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256'
```

```

6-GCM-SHA384:ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-D
SS-AES128-GCM-SHA256:kEDH+AESGCM:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES12
8-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:ECDHE-RSA-AES256-SHA3
84:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:D
HE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES2
56-SHA256:DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:AES128-GCM-SHA256:AES256-G
CM-SHA384:AES128-SHA256:AES256-SHA256:AES128-SHA:AES256-SHA:AES:CAMELLIA:D
ES-CBC3-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!MD5:!PSK:!aECDH:!EDH-DSS-DES-
CBC3-SHA:!EDH-RSA-DES-CBC3-SHA:!KRB5-DES-CBC3-SHA';
    ssl_dhparam /etc/ssl/private/dhparams.pem;

ssl_prefer_server_ciphers on;
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) {
        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](#)
- [Configuration](#)
- [User Set-Up](#)

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 Azure MFA

- [Introduction](#)
- [Configuring Azure MFA for Awingu](#)
- [Configuring Awingu for Azure MFA](#)

Introduction

Awingu integrates with Azure MFA for multi-factor authentication.

This guide will walk you through the different steps required to configure both Awingu and Azure MFA to enable the integration.

Configuring Azure MFA for Awingu

Awingu leverages the Microsoft *Azure Multi-Factor Authentication Server* to integrate Azure MFA. Step-by-step instructions can be found here: <https://azure.microsoft.com/en-us/documentation/articles/multi-factor-authentication-get-started-server/>

Awingu will connect to the Azure Multi-Factor Authentication Server using *Azure MFA Server Mobile App Web Service*. Step-by-step instructions can be found here:

<https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-get-started-server-webservice>

Configuring Awingu for Azure MFA

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 *Azure MFA* mode. Following configuration options appear, which values are configured during the setup of the *Azure MFA Server Mobile App Web Service*.

- **SDK url:** Typically in the form of <https://my-mfa-server/MultiFactorAuthWebServiceSdk/>
- **SDK username:** Named WEB_SERVICE_SDK_AUTHENTICATION_USERNAME in the Web Service setup.
- **SDK password:** Named WEB_SERVICE_SDK_AUTHENTICATION_PASSWORD in the Web Service setup.
- **LDAP Username Attribute:** can be kept to sAMAccountName.

Press *Apply* and Awingu is configured to use *Azure MFA* as MFA provider for all users of the selected domain.

Integrating Awingu with DUO

- [Introduction](#)
- [Prerequisites](#)
- [Configuring your Awingu application in Duo](#)
- [Configuring Duo in Awingu](#)
- [Users](#)
- [Known Limitations](#)

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.

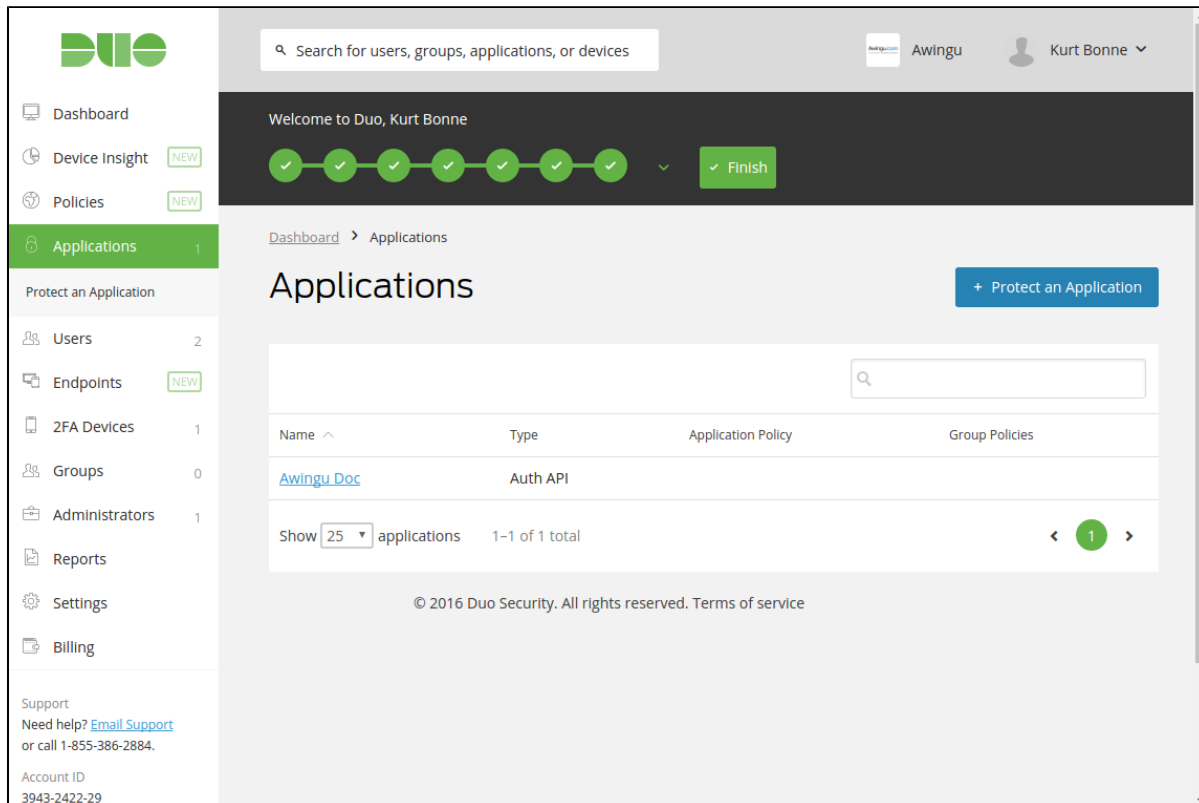
Prerequisites

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.

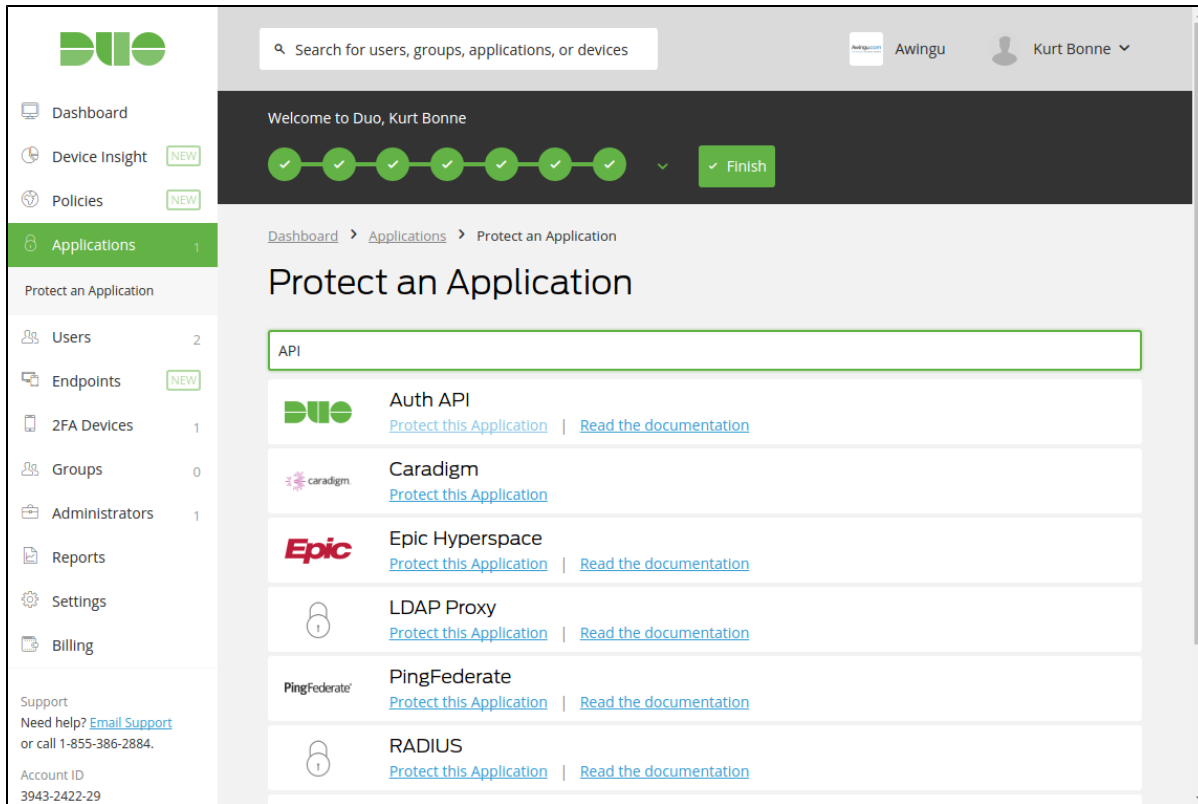
As Duo is a SaaS service, the Awingu environment requires access to the Duo SaaS service. This is TCP 443 to the API hostname of your configured application (<your_api>.duosecurity.com).

Configuring your Awingu application in Duo

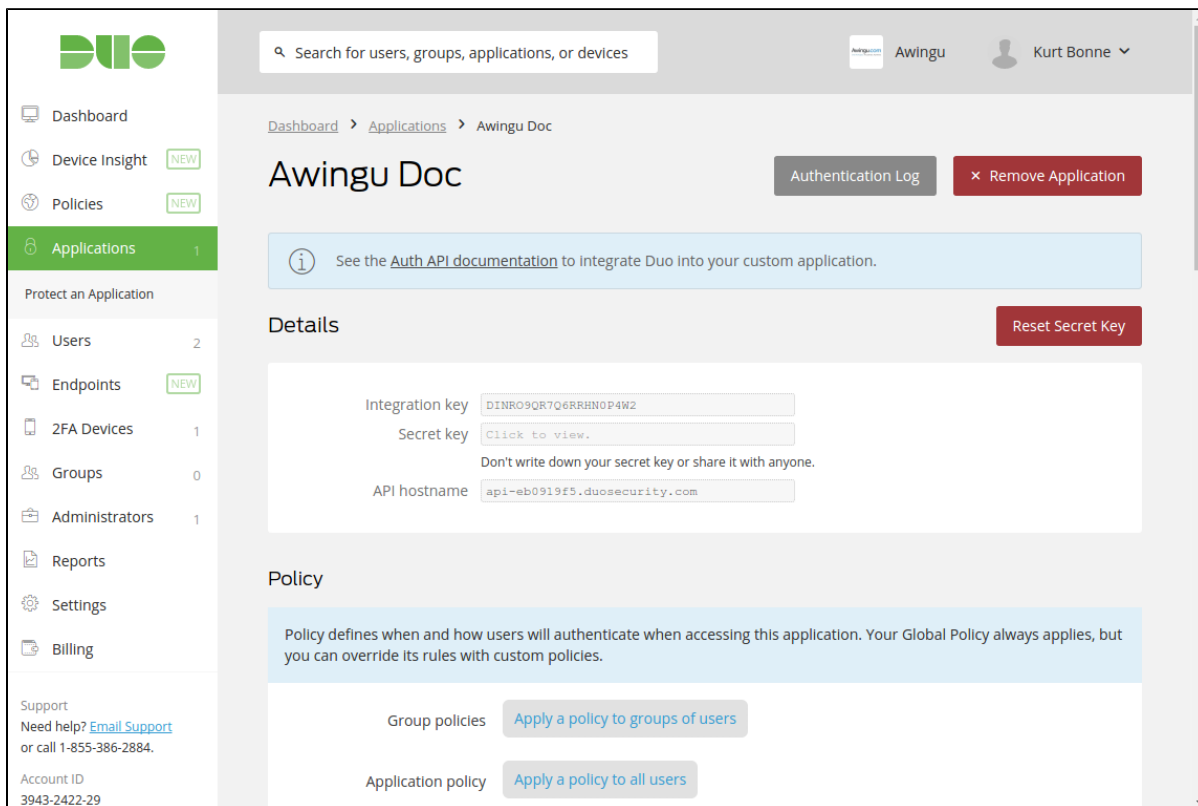
Sign-in to your Duo account and select **Applications** in the menu.



To add your Awingu application, click *Protect an Application* and select *Auth API* as type.



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.



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**

"DOMAINusername", "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.

✓ Save Changes

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.

DEV-AWINGU
Configure
Manage
Global
Apply Changes

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
------	-------

System Management Console - © 2012-2016 Awingu N.V. - Eula
3.3

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 by setting the user's status to *bypass*. Awingu does not honour this status and thus will prevent the user to sign in.

Single Sign-On for SaaS Applications

Single Sign-On for Azure AD - Office 365

- [Introduction](#)
- [Preparations](#)
- [Setting up Awingu as Identity Provider](#)
- [Configure Exchange to use Awingu as Identity Provider](#)
- [Configure Skype for business to use Awingu as Identity Provider](#)
- [Configuring Azure AD to use Awingu as Identity Provider](#)
- [Adding Office 365 Apps to Awingu](#)
- [Use Azure AD as IdP Proxy](#)

Introduction

Azure Active Directory (Azure AD) is the authentication service for Office 365.

Integrating Single Sign-On (SSO) for Microsoft Azure AD / Office 365 into Awingu enables following behavior:

- Once signed-in to Awingu, you can open Office 365 OneDrive, Word, Excel, PowerPoint etc. directly via Awingu without additional log-in.
- To sign-in to Office 365 OneDrive, Word, Excel, PowerPoint etc., you will be redirected to Awingu, where you need to sign-in with your Awingu credentials.

Awingu serves as Identity Provider (IdP), as defined in SAML V2.0. This means that Azure AD will always check with Awingu if a user is allowed to sign-in to its services.

When Awingu is not accessible for the end-user, (s)he won't be able to sign-in to Azure AD / Office 365.

There is no auto sign-out. Users still need to sign-out from both Awingu and Azure AD / Office 365 separately.

For more in-depth technical information, please refer to [MSDN Documentation about Azure](#).

Preparations

Verifying your domain

To be able to use Awingu as IdP for Office 365, you will need to verify ownership of the domain for which you want to implement SSO (e.g. mycompany.com). More information can be found on [Azure's documentation portal](#).

Sourcing Azure AD with your Domain Controller

Awingu can only serve as Identity Provider (IdP) for Azure AD if the users are sourced from your (local) Domain Controller.

- **Azure AD Connect** integrates your on-premises Domain Controller with Azure AD. This allows you to provide a common identity for your users for Office 365, Azure, and SaaS applications integrated with Azure AD. More information can be found on [Azure's documentation portal](#).
- **PowerShell** can be used to automate adding new users to Azure AD and to synchronize changes from the on-premises directory. You must download the Windows Azure Active Directory Modules which can be obtained here: <http://technet.microsoft.com/library/jj151815.aspx>

Setting up Awingu as Identity Provider

Awingu is configured as IdP via the [User Connector](#) section in the System Settings.

System Settings > Configure > User Connector > SSO Identity Provider (IdP)

- **State:** Enable or Disable IdP functionality in Awingu for all SaaS services.
- **Issuer:** URL from which Awingu is reachable for the end-users, e.g. <https://awingu.mycompany.com/>.
- **Logout URL:** The logout URL redirects the browser to this URL, once the user logs out of the SaaS application that is configured for SSO. By default, the Logout URL is '/' (i.e goes to Awingu main page), but it can hold any valid URL.

SAML V2.0 mandates that responses are cryptographically signed. Awingu uses a certificate and private key to generate the SAML responses. The SaaS service validates the response with the certificate, which should be configured in the service. As there is no certificate authority involved, the certificate can be self signed. Note that the certificate-key pair is the same for all configured SaaS services configured within one Awingu domain.

- **Certificate:** The public X.509 certificate for the provided Issuer in **.crt format/.pem format**, ASCII file, starting with:
-----BEGIN CERTIFICATE-----
- **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-----

The way you generate keys and certificates often depends on your development platform and programming language preference. Here an example is shown how to generate a certificate using [openssl](#) (download for Windows [here](#)) via the command line:

```
set OPENSSL_CONF=C:/OpenSSL-Win32/bin/openssl.cfg
C:\OpenSSL-Win32\bin\openssl.exe genrsa -out private_key.pem 2048
C:\OpenSSL-Win32\bin\openssl.exe req -new -x509 -days 3650 -key
private_key.pem -out certificate.pem
```

When the "Common Name" is asked, please enter your domain name, e.g. [mycompany.com](#).

An alternative way to generate keys: https://www.samltool.com/self_signed_certs.php (note: generating keys via a third party always induces a security risk).

Security Warning

The private key should be kept secret at all times. If this key gets compromised, unauthorized individuals can access to your corporate accounts of the SaaS services.

System Settings > Configure > User Connector > SSO Services

Select *Azure AD / Office 365* in the list of Services and the pane *SSO Service Details* will appear below the table.

- **State:** Enable/disable SSO for Azure AD / Office 365
- **ACS URL:** Keep the default value <https://login.microsoftonline.com/login.srf>
- **Issuer:** Keep the default value `urn:federation:MicrosoftOnline`

Configure Exchange to use Awingu as Identity Provider

1. Start Powershell with admin rights
2. Windows PowerShell needs to be configured to run scripts, and by default, it isn't:

```
Set-ExecutionPolicy RemoteSigned
```

3. Startup a new session towards Exchange online

```
$credential = Get-Credential

$Session = New-PSSession -ConfigurationName Microsoft.Exchange
-ConnectionUri https://outlook.office365.com/powershell-liveid/
-Credential $UserCredential -Authentication Basic -AllowRedirection

Import-PSSession $session
```

4. Enable OAuth authentication for the tenant

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
Get-OrganizationConfig | Format-Table -Auto Name,OAuth*
```

Configure Skype for business to use Awingu as Identity Provider

1. Download and install the skype for business powershell module from <https://www.microsoft.com/en-us/download/details.aspx?id=39366>
2. Start Powershell with admin rights

```
Import the module:  
Import-Module LyncOnlineConnector
```

3. Windows PowerShell needs to be configured to run scripts, and by default, it isn't:

```
Set-ExecutionPolicy RemoteSigned
```

4. Start a new session towards Skype For Business

```
$credential = Get-Credential  
$session = New-CsOnlineSession -Credential $credential  
Import-PSSession $session
```

5. Enable ADAL authentication for the tenant

```
Enable ADAL authentication for the tenant  
Set-CsOAuthConfiguration -ClientAdalAuthOverride Allowed  
Get-CsOAuthConfiguration
```

Configuring Azure AD to use Awingu as Identity Provider

In order to configure Azure AD / Office 365 for SSO, the following steps need to be taken:

1. Download the Windows Azure Active Directory Modules from here: <http://technet.microsoft.com/library/jj151815.aspx>
2. Open *Windows Azure Active Directory module for PowerShell*. A new PowerShell window is opened.
3. Execute following commands, but substitute:
 - a. `<issuer_url>` is the URL from which the Awingu environment is reachable, e.g. <https://awingu.mycompany.com>
 - b. `<domain_name>` is the domain name linked to Azure AD, e.g. `mycompany.com`
 - c. `<certificate>` is the public certificate (the same as [provided to Awingu](#)). Only enter the characters between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- without spaces. Example:

```
-----BEGIN CERTIFICATE-----  
MIIDjzCCAnegAwIBAgIJAMcwwqO+NeE8MA0GCSqGSIb3DQEBCwUAMF4xCzAJBgNV  
BAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXR1MSEwHwYDVQQKBhJbnRlcm5ldCBX  
aWRnaXRzIFB0eSBMdGQxRzAVBgNVBAMMDmRldi1hd2luZ3UuY29tMB4XDTE2MDYx  
-----END CERTIFICATE-----
```

becomes:

```
MIIDjzCCAnegAwIBAgIJAMcwwqO+NeE8MA0GCSqGSIb3DQEBCwUAMF4xCzAJBgNV  
BAYTAkFVMRMwEQYDVQQIDApTb211LVN0YXR1MSEwHwYDVQQKBhJbnRlcm5ldCBX  
aWRnaXRzIFB0eSBMdGQxRzAVBgNVBAMMDmRldi1hd2luZ3UuY29tMB4XDTE2MDYx
```

```

Import-Module MSOnline
Connect-MsolService
$dom = "<domain_name>"
$LogOnUrl = "<issuer_url>/idp/login"
$LogOffUrl = "<issuer_url>/idp/logout"
$uri = "<issuer_url>/" # important to put the trailing slash
here!
$MySigningCert = "<certificate>"
Set-MsolDomainAuthentication -DomainName $dom -FederationBrandName
$dom -Authentication Federated -PassiveLogOnUri $LogOnUrl
-SigningCertificate $MySigningCert -IssuerUri $uri -LogOffUri
$LogOffUrl -PreferredAuthenticationProtocol SAMLp

```

4. You can verify with:

```

Connect-MsolService
Get-MsolDomainFederationSettings -domainname:<domain_name>

```

Sync between local AD and Azure active directory

1. Prepare for single sign-on (verify requirements)
2. Install the Windows Azure Active Directory Module for Windows PowerShell (we will not use ADFS)
3. Verify additional domains
4. Prepare for directory synchronization (verify requirements)
5. Activate Active Directory@ synchronization
6. Install and configure the Directory Sync tool (Syncs on Premise AD accounts with Azure AD for Office 365)
7. Verify directory synchronization
8. Activate synchronized users
9. Verify and manage single sign-on

Microsoft provides a detailed Implementer's Guide for Office 365 SAML2.0 integration [Download doc here](#).

Adding Office 365 Apps to Awingu

Office 365 Apps can be added as web applications to Awingu in System Settings > Manage > Applications:

- **Name:** The application name as it will appear in the Awingu user interface, e.g. Office 365 Portal.
- **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. Please use PNG or JPG format.
- **Protocol:** Select *Web Application*.
- **Command:** `https://login.microsoftonline.com/login.srf?wa=wsignin1.0&whr=<domain_name>&wreply=<redirection_url>`
 - `<domain_name>` is the domain name linked to Azure AD, e.g. `mycompany.com`
 - `<redirection_url>` is the URL of the application you want to open (URL encoded):

Office 365 App	<redirection_url>
Office 365 Portal	<code>https%3A%2F%2Fportal.office.com%2F</code>
Office 365 Mail	<code>https%3A%2F%2Foutlook.office.com%2Fowa%2F</code>
OneDrive	<code>https%3A%2F%2F<sharepoint_domain>-my.sharepoint.com%2F_layouts%2F15%2FMySite.aspx%3FMySiteRedirect%3DAIldocuments</code>
Word Online	<code>https%3A%2F%2Foffice.live.com%2Fstart%2FWord.aspx%3Fauth%3D2</code>
Excel Online	<code>https%3A%2F%2Foffice.live.com%2Fstart%2FExcel.aspx%3Fauth%3D2</code>

PowerPoint Online	https%3A%2F%2Foffice.live.com%2Fstart%2FPowerPoint.aspx%3Fauth%3D2
-------------------	--

- **Categories:** Associate zero, one or more application categories to this application.
- **Media Types:** Keep empty: not applicable for web applications.
- **Labels:** Add labels to applications to group them. These groups can be used to filter application servers in lists and reports.
- **Server Labels:** Keep empty: not applicable for web applications.
- **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 [Application Management](#) for more details.

User labels in Awingu only affects whether the application is shown for the user. If the user has valid credentials for Office 365 apps, (s)he still will be able to use the application.

Use Azure AD as IdP Proxy

To support single sign-on (SSO) for other SaaS services than the ones supported by Awingu, like Citrix GoToMeeting, Facebook At Work, etc., you can use Azure Active Directory (Azure AD) as IdP Proxy.

This enables following behavior:

- Once signed-in to Awingu, you can open the SaaS service directly via Awingu without entering credentials of Azure AD, nor the ones of the SaaS service.
- To sign-in to the SaaS service, you will be redirected to Awingu, where you need to sign-in with your Awingu credentials.

When accessing such a SaaS services, following steps happen:

- The SaaS service redirects the user to Azure AD, which serves as an Identity Provider (IdP) for that SaaS service.
- Azure AD redirects the user to Awingu, which serves as an Identity Provider (IdP) for Azure AD, as defined in SAML 2.0.
- Awingu identifies the user. If the user is not signed in, the Awingu log-in screen appears.
- After successful identification, Awingu redirects back to Azure AD
- Azure redirects the user back to the original SaaS service.

To use Azure AD as IdP proxy for Awingu, you need first to set-up SSO for Azure AD, as described in the previous sections.

Adding SaaS Services on Azure AD

SaaS services are called Applications on Azure AD.

1. In the [Azure classic portal](#), on the left navigation pane, click **Active Directory**.
2. From the **Directory** list, select the directory that you would like to add Salesforce to.
3. Click on **Applications** in the top menu.
4. Click **Add an application from the gallery**.
5. Search for your desired application, e.g. Citrix GoToMeeting, Facebook At Work, etc.
6. Select the desired application and click on the complete button on the lower right.
7. You should now see the Quick Start page for the application.
8. Click the **Configure single sign-on** button.
9. Select **Azure AD Single Sign-On**, and then click **Next**.
10. Follow the steps of the wizard.
11. Once the SSO is configured, click on **Dashboard** in the top menu of the corresponding application.
12. On the bottom right, you will find the **Single Sign-On URL**. Note this for the next section.

More details for all supported applications can be found on [documentation portal of Azure](#).

Adding the SaaS Service as Application to Awingu

The added SaaS service can be added as web applications to Awingu in System Settings > Manage > Applications:

- **Name:** The application name as it will appear in the Awingu user interface, e.g. Citrix GoToMeeting, Facebook At Work, etc.
- **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. Please use PNG or JPG format.
- **Protocol:** Select *Web Application*.
- **Destination URL:** Enter the **Single Sign-On URL** from the previous section.
- **Reverse Proxy:** Disabled.
- **Categories:** Associate zero, one or more application categories to this application.
- **Media Types:** Keep empty: not applicable for web applications.
- **Labels:** Add labels to applications to group them. These groups can be used to filter application servers in lists and reports.
- **Server Labels:** Keep empty: not applicable for web applications.

- **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 [Application Management](#) for more details.

When opening the application in Awingu while not being signed-in to Azure, you will first reach the Azure login page.

- If you have used your Azure account before on that browser, you can just click on your username to continue.
- If it is the first time you have used your Azure account on that browser, you just need to fill-in your username after which you should automatically be redirected.

User labels in Awingu only affects whether the application is shown for the user. If the user has valid credentials for the SaaS services, (s)he still will be able to use the application.

Single Sign-On for Google Apps

- [Introduction](#)
- [Preparations](#)
- [Setting up Avingu as Identity Provider](#)
- [Configuring Google Apps to use Avingu as Identity Provider](#)
- [Adding Google Applications to Avingu](#)

Introduction

Integrating Single Sign-On (SSO) for Google Apps for Work into Avingu enables following behavior:

- Once signed-in to Avingu, you can open Google Mail, Google Drive, Google Sheets etc. directly via Avingu without additional log-in.
- To sign-in to Google Mail, Google Drive, Google Sheets etc., you will be redirected to Avingu, where you need to sign-in with your Avingu credentials.

Avingu serves as Identity Provider (IdP), as defined in SAML V2.0. This means that Google Apps will always check with Avingu if a user is allowed to sign-in to its services.

When Avingu is not accessible for the end-user, (s)he won't be able to sign-in to Google Apps.

There is no auto sign-out. Users still need to sign-out from both Avingu and Google Apps separately.

For more in-depth technical information, please refer to [Google's documentation for SSO integration](#).

Preparations

Set-up your domain for Google Apps

To be able to use Avingu as IdP for Google Apps domain, you need Google Apps for Work to be set-up and verified for your domain (e.g. for mycompany.com) on <https://apps.google.com/>


To access the Admin Console, you can browse to <https://www.google.com/a/<account>>, with <account> the account domain name configured at Google Apps, e.g. <https://www.google.com/a/mycompany.com>

Link your Google Apps accounts with the users on the Active Directory

In order to configure SSO for Google Apps, you'll need to make sure every user has an Active Directory (or LDAP) account that maps onto a Google Apps account. Avingu uses the e-mail address (*mail* attribute) configured on the AD as account name for Google Apps. In case the e-mail address is not provided, the UPN is used.

Sam Lovely Properties ? x

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile	COM+	Attribute Editor		
General	Address	Account	Profile	Telephones
Organization				

 Sam Lovely

First name: Initials:


Last name:

Display name:




Description:

Office:


Telephone number:


E-mail: 

Web page:

Google Search for users, groups, and settings (e.g. cannot login)   

Users > Sam Lovely ? :



Sam Lovely
sam.lovely@mycompany.com 
Super Admin · Active
Last login 11:51 PM PDT

0 GB
Mail storage used

1
Docs owned

Account
View and manage profile, security, aliases, and usage stats.

8 Google Apps enabled
View active Google apps and services.

[SEND FEEDBACK](#)

If you already have your user accounts in your Active Directory, you can sync them with your Google Apps domain using **Google Apps Directory Sync (GADS)**. GADS is a versatile utility that you can use to synchronize user accounts between your Google Apps domain and your AD server. Using GADS you can automatically add, modify, and delete users, groups, and non employee contacts to synchronize the data in your Google Apps domain with your LDAP directory server (Active Directory Server). The data in your LDAP directory server is never modified or compromised. GADS is a secure tool that help you easily keep track of users and groups.

The GADS Configuration Manager is quite versatile and allows you to customize synchronizations. Before you perform the actual synchronization, you can simulate test synchronizations to find what works best for your organization and then schedule synchronizations to occur when you need

them.

For more information about GADS, please see <https://support.google.com/a/topic/2679497>.

Example: although each directory sync depends on specific AD and Google Apps settings, a few essential synchronization steps are shown below:

1. Configure connectivity with your LDAP server

The screenshot shows the 'Google Apps Directory Sync' application window. The 'Connection Settings' tab is active. The left sidebar contains a menu with options: General Settings, Google Apps Configuration, LDAP Configuration (highlighted), Org Units, User Accounts, Groups, User Profiles, Shared Contacts, Calendar Resources, Notifications, Logging, and Sync. The main area contains the following settings:

- Server Type: MS Active Directory
- Connection Type: Standard LDAP
- Host Name: 172.28.0.5
- Port: 389
- Authentication Type: Simple
- Authorized User: AWINGU\admin
- Password: (masked with dots)
- Base DN: dc=my,dc=awingu,dc=com

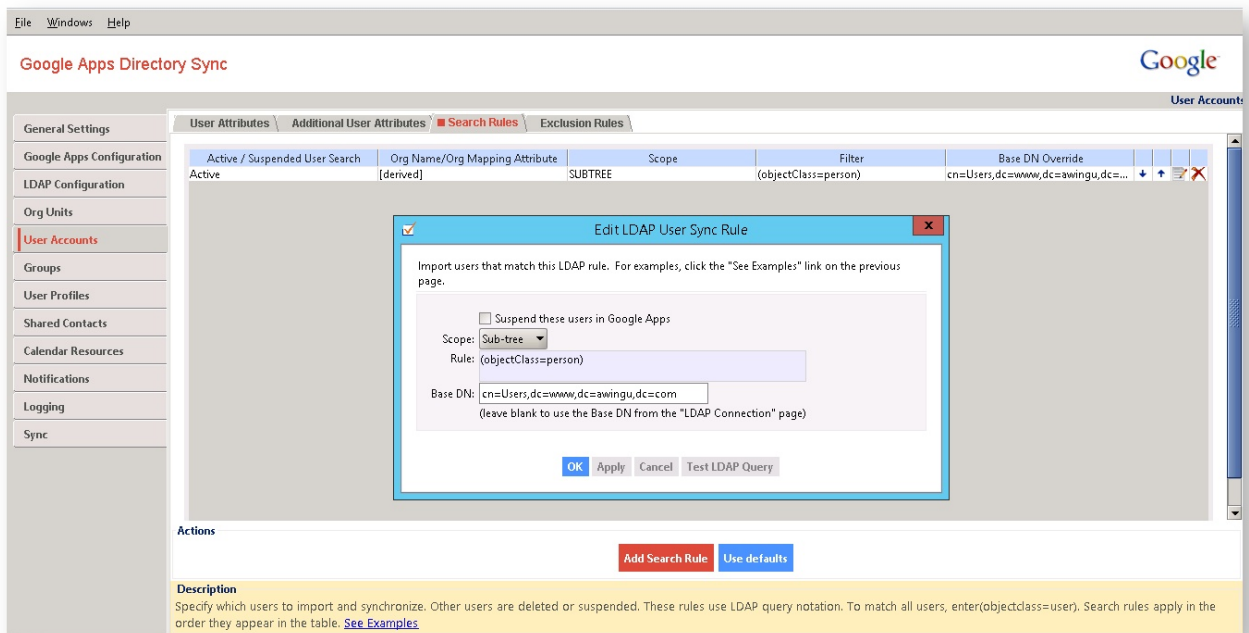
2. Specify which organization unit (OU) you want to map to Google App unit names

The screenshot shows the 'Google Apps Directory Sync' application window with the 'LDAP Org Unit Mappings' tab selected. The left sidebar is the same as in the previous screenshot. The main area shows the 'Synchronization of Google Organizations (from LDAP Org Units)' section. A checkbox is present with the text: 'Do not create or delete Google Organizations, but move users between existing Organizations, as specified in the User Sync Rules'. Below this is a table with two columns: 'LDAP DN' and 'Google Org Unit Name'. The first row shows 'CN=Users,dc=www,dc=awingu,dc=com' and 'Awingu-Users'. An 'Edit Mapping from LDAP DN to Google Apps Org Name' dialog box is open over the table. The dialog box contains the following text and fields:

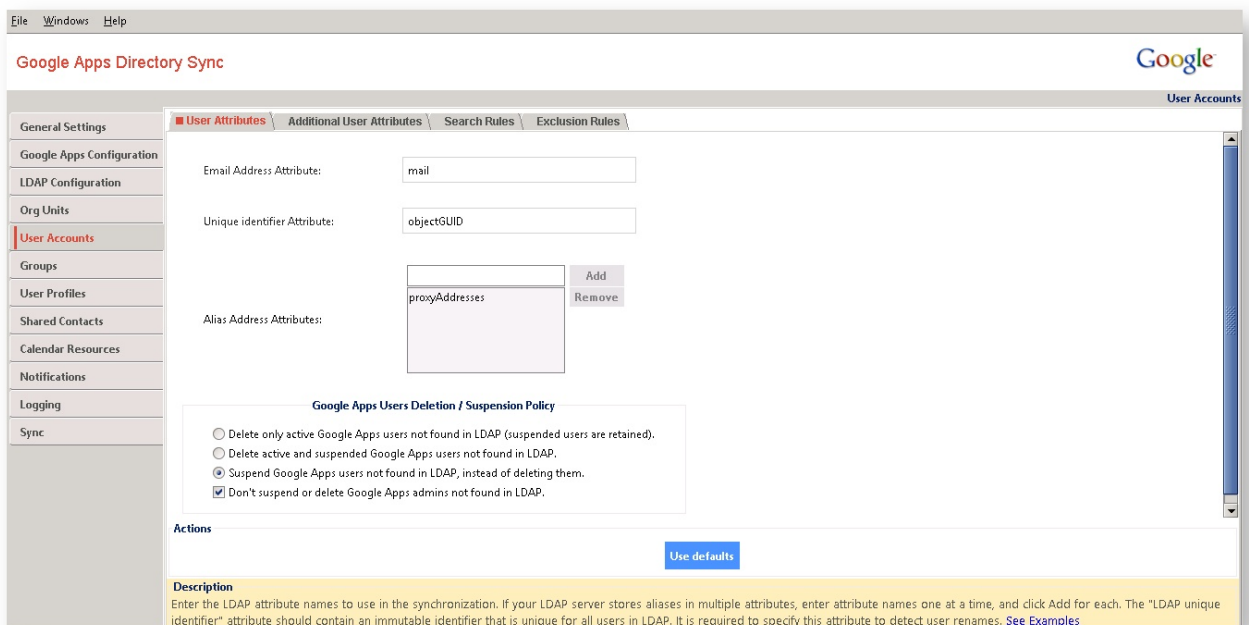
- Specify the full LDAP DN (example: ou=users,dc=example,dc=com) and the corresponding Google Apps Org Unit name (example: users).
- (LDAP) DN: CN=Users,dc=www,dc=awingu,dc=com
- (Google Apps) Name: Awingu-Users
- Buttons: OK, Apply, Cancel

At the bottom of the main window, there is an 'Actions' section with an 'Add Mapping' button and a 'Description' section with text explaining how to specify OUs and map them to Google Apps Org Units.

3. Specify an LDAP search query to select the users you want to synchronize



4. Specify the user attribute you want to synchronize. Every Google Appss user account needs to be linked to an email address. You can synchronize an existing email address from an AD user using the *mail* attribute. E-mail aliases (to be used in Google Mail) can be synchronized by mapping the *proxyAddresses* attribute.



Setting up Awingu as Identity Provider

Awingu is configured as IdP via the [User Connector](#) section in the System Settings.

System Settings > Configure > User Connector > SSO Identity Provider (IdP)

- **State:** Enable or Disable IdP functionality in Awingu for all SaaS services.
- **Issuer:** URL from which Awingu is reachable for the end-users, e.g. <https://awingu.mycompany.com/>.
- **Logout URL:** The logout URL redirects the browser to this URL, once the user logs out of the SaaS application that is configured for SSO. By default, the Logout URL is '/' (i.e goes to Awingu main page), but it can hold any valid URL.

SAML V2.0 mandates that responses are cryptographically signed. Awingu uses a certificate and private key to generate the SAML responses.

The SaaS service validates the response with the certificate, which should be configured in the service. As there is no certificate authority involved, the certificate can be self signed. Note that the certificate-key pair is the same for all configured SaaS services configured within one Awingu domain.

- **Certificate:** The public X.509 certificate for the provided Issuer in **.crt format/.pem format**, ASCII file, starting with:
-----BEGIN CERTIFICATE-----
- **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-----

The way you generate keys and certificates often depends on your development platform and programming language preference. Here an example is shown how to generate a certificate using [openssl](#) (download for Windows [here](#)) via the command line:

```
set OPENSSL_CONF=C:/OpenSSL-Win32/bin/openssl.cfg
C:\OpenSSL-Win32\bin\openssl.exe genrsa -out private_key.pem 2048
C:\OpenSSL-Win32\bin\openssl.exe req -new -x509 -days 3650 -key
private_key.pem -out certificate.pem
```

When the "Common Name" is asked, please enter your domain name, e.g. [mycompany.com](#).

An alternative way to generate keys: https://www.samltool.com/self_signed_certs.php (note: generating keys via a third party always induces a security risk).

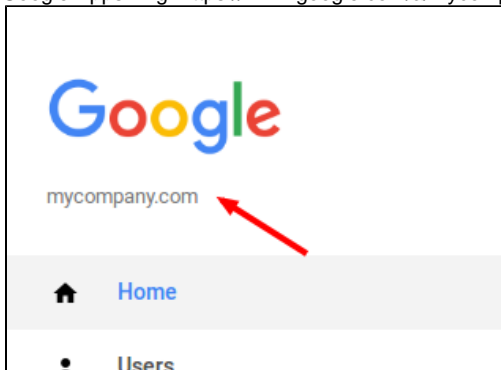
Security Warning

The private key should be kept secret at all times. If this key gets compromised, unauthorized individuals can access to your corporate accounts of the SaaS services.

System Settings > Configure > User Connector > SSO Services

Select *Google Apps* in the list of Services and the pane *SSO Service Details* will appear below the table.

- **State:** Enable/disable SSO for Google Apps
- **ACS URL:** Enter following URL: <https://www.google.com/a/<account>/acs>, with <account> the account domain name configured at Google Apps. E.g. <https://www.google.com/a/mycompany.com/acs>



Configuring Google Apps to use Awingu as Identity Provider

In order to configure Google Apps for SSO, the following steps need to be taken:

1. Login to the **Admin Console** of your Google Apps for Work domain: <https://www.google.com/a/<account>>, with <account> the account domain name configured at Google Apps, e.g. <https://www.google.com/a/mycompany.com>
2. Go to **Security > Set up single sign-on (SSO)**
3. Enable **Setup SSO with third party identity provider** and fill-in following fields.
Note: <issuer_url> is the URL from which the Awingu environment is reachable, e.g. <https://awingu.mycompany.com>
 - a. **Sign-in page URL:** <issuer_url>/idp/login. E.g. <https://awingu.mycompany.com/idp/login>
 - b. **Sign-out page URL:** <issuer_url>/idp/logout. E.g. <https://awingu.mycompany.com/idp/logout>
 - c. **Change password URL:** not supported, but cannot be left blank. Enter <issuer_url>
 - d. **Verification certificate:** Upload your your public certificate. This is the same as [provided to Awingu](#).
4. Click on **Save**.

Adding Google Applications to Awingu

The Google Applications can be added to Awingu as any web application in System Settings > Manage > Applications:

- **Name:** The application name as it will appear in the Awingu user interface, e.g. Google Mail.
- **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. Please use PNG or JPG format.
- **Protocol:** Select *Web Application*.
- **Destination URL:** Enter the corresponding URL, with <account> the account domain name configured at Google Apps, e.g. [mycompany.com](https://mail.google.com/a/mycompany.com).

Google App	URL
Google Mail	<a href="https://mail.google.com/a/<account>">https://mail.google.com/a/<account>
Google Calendar	<a href="https://calendar.google.com/a/<account>">https://calendar.google.com/a/<account>
Google Drive	<a href="https://drive.google.com/a/<account>">https://drive.google.com/a/<account>
Google Docs	<a href="https://docs.google.com/a/<account>">https://docs.google.com/a/<account>
Google Sheets	<a href="https://sheets.google.com/a/<account>">https://sheets.google.com/a/<account>
Google Slides	<a href="https://slides.google.com/a/<account>">https://slides.google.com/a/<account>
Google Groups	<a href="https://groups.google.com/a/<account>">https://groups.google.com/a/<account>
Google Sites	<a href="https://sites.google.com/a/<account>">https://sites.google.com/a/<account>

- **Reverse Proxy:** Disabled.
- **Categories:** Associate zero, one or more application categories to this application.
- **Media Types:** Keep empty: not applicable for web applications.
- **Labels:** Add labels to applications to group them. These groups can be used to filter application servers in lists and reports.
- **Server Labels:** Keep empty: not applicable for web applications.
- **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 [Application Management](#) for more details.

User labels in Awingu only affects whether the application is shown for the user. If the user has valid credentials for Google Apps, (s)he still will be able to use the application.

Single Sign-On for Okta

- [Introduction](#)
- [Linking Okta users with AD](#)
- [Setting up Awingu as Identity Provider](#)
- [Configuring Okta to use Awingu as Identity Provider](#)
 - [Inbound SAML](#)
 - [JIT Provisioning](#)
- [Configure Awingu to Enable SSO for Okta](#)
- [Adding Okta Applications to Awingu](#)

Introduction

To support single sign-on (SSO) for other SaaS services than the ones supported by Awingu, like Citrix GoToMeeting, Facebook At Work, etc., you can use Okta as **IdP Proxy** (Identity Provider Proxy).

This enables following behavior:

- Once signed-in to Awingu, you can open the SaaS service directly via Awingu without additional log-in.
- To sign-in to the SaaS service, you will be redirected to Awingu, where you need to sign-in with your Awingu credentials.

There is no auto sign-out. Users still need to sign-out from both Awingu, Okta and the SaaS service separately. Awingu and Okta sign-out the users after a certain inactivity time.

When accessing such a SaaS services, following steps happen:

- The SaaS service redirects the user to Okta, which serves as an Identity Provider (IdP) for that SaaS service.
- Okta redirects the user to Awingu, which serves as an Identity Provider (IdP) for Okta, as defined in SAML 2.0.
- Awingu identifies the user. If the user is not signed in, the Awingu log-in screen appears.
- After successful identification, Awingu redirects back to Okta
- Okta redirects the user back to the original SaaS service.

In Okta, SaaS services are called *Applications*.


For more in-depth technical information, please refer to [the Okta Help Center](#).

Linking Okta users with AD

In order to configure SSO for Okta, you'll need to make sure every user has an Active Directory (or LDAP) account that maps onto an Okta account. Awingu uses the e-mail address (*mail* attribute) configured on the AD as account name for Okta. In case the e-mail address is not provided, the UPN is used.

Sam Lovely Properties ? x

Published Certificates	Member Of	Password Replication	Dial-in	Object
Security	Environment	Sessions	Remote control	
Remote Desktop Services Profile	COM+	Attribute Editor		
General	Address	Account	Profile	Telephones
Organization				

 Sam Lovely

First name: Initials:


Last name:

Display name:

Description:



Office:

Telephone number:

E-mail: 



Web page:

Okta Dashboard Directory Applications Security Reports

 **Sam Lovely** 
sam.lovely@mycompany.com
Active

Applications Groups Profile

Assigned Applications

Application	Assignment & App Username	
 UptimeRobot	Individual sam.lovely@mycompany.com	<input type="button" value="Edit"/> <input type="button" value="Remove"/>
 Salesforce.com	Individual sam.lovely@mycompany.com	<input type="button" value="Edit"/> <input type="button" value="Remove"/>

If you already have your user accounts in your Active Directory, you can:

- Sync them with your Okta account using the **Okta Active Directory Agent**. Detailed instructions can be found on [the Okta Help Center](#).
- Use Just-In-Time (JIT) provisioning. Users are auto-added to Okta the first time they access a SaaS service via Awingu through Okta (see section [JIT Provisioning](#)).

Setting up Awingu as Identity Provider

Awingu is configured as IdP via the [User Connector](#) section in the System Settings.

Go to System Settings > Configure > User Connector > SSO Identity Provider (IdP)

- **State:** Enable or Disable IdP functionality in Awingu for all SaaS services.
- **Issuer:** URL from which Awingu is reachable for the end-users, e.g. <https://awingu.mycompany.com/>.
- **Logout URL:** The logout URL redirects the browser to this URL, once the user logs out of the SaaS application that is configured for SSO. By default, the Logout URL is '/' (i.e goes to Awingu main page), but it can hold any valid URL.

SAML V2.0 mandates that responses are cryptographically signed. Awingu uses a certificate and private key to generate the SAML responses. The SaaS service validates the response with the certificate, which should be configured in the service. As there is no certificate authority involved, the certificate can be self signed. Note that the certificate-key pair is the same for all configured SaaS services configured within one Awingu domain.

- **Certificate:** The public X.509 certificate for the provided Issuer in **.crt format/.pem format**, ASCII file, starting with:
-----BEGIN CERTIFICATE-----
- **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-----

The way you generate keys and certificates often depends on your development platform and programming language preference. Here an example is shown how to generate a certificate using [openssl](#) (download for Windows [here](#)) via the command line:

```
set OPENSSL_CONF=C:/OpenSSL-Win32/bin/openssl.cfg
C:\OpenSSL-Win32\bin\openssl.exe genrsa -out private_key.pem 2048
C:\OpenSSL-Win32\bin\openssl.exe req -new -x509 -days 3650 -key
private_key.pem -out certificate.pem
```

When the "Common Name" is asked, please enter your domain name, e.g. [mycompany.com](#).

An alternative way to generate keys: https://www.samltool.com/self_signed_certs.php (note: generating keys via a third party always induces a security risk).

Security Warning

The private key should be kept secret at all times. If this key gets compromised, unauthorized individuals can access to your corporate accounts of the SaaS services.

Configuring Okta to use Awingu as Identity Provider

Inbound SAML

In order to configure Okta for SSO, the following steps need to be taken:

1. As Okta Administrator, login to your Okta account and click on **Admin**.
2. On the top menu, go to **Security > Authentication**.
3. Go to the **Inbound SAML** section.
4. Click on **Add Endpoint** and fill-in following data:
 - <issuer_url> the URL from which the Awingu environment is reachable. E.g. <https://awingu.mycompany.com>
 - a. **IDP Certificate:** Upload your public certificate. This is the same as provided to Awingu.
 - b. **IDP Issuer:** <issuer_url>. Note the trailing slash, e.g. <https://awingu.mycompany.com/>
 - c. **IDP Login URL:** <issuer_url>/idp/login, e.g. <https://awingu.mycompany.com/idp/login>
 - d. **IDP Binding:** HTTP-Post
 - e. **Default Group Assignment:** (optional) New users will be added to the group when JIT provisioning (auto-creation of Okta users) is enabled.
 - f. **Transform Username:** username
 - g. **Name ID Format:** Email Address
 - h. **Enable SP initiated SAML:** enable this to auto-redirect to Awingu.

When Awingu is not accessible for the end-user, (s)he won't be able to sign-in via Okta. There is a workaround by using the link mentioned in the form. Note that when the user has no Okta credentials (e.g. because of JIT provisioning), (s)he won't have this workaround.

5. Click on **Save Endpoint**.
6. Note down the 2 shown URLs needed for next section [Configure Awingu to enable SSO for Okta](#):
 - a. *Assertion Consumer Service*
 - b. *Audience URI*

JIT Provisioning

To auto-create users in Okta the first time they access Okta via Awingu:

1. As Okta Administrator, login to your Okta account and click on **Admin**.
2. On the top menu, go to **Security > Authentication**.
3. Go to the **JIT Provisioning** section.
4. Click on **Edit** to Enable Just In Time Provisioning.

Note that users created via JIT won't have an Okta password and can only use Okta via Awingu.
Note that the First name, Last name, User name and E-mail should be configured on the AD.

Configure Awingu to Enable SSO for Okta

Go to System Settings > Configure > User Connector > SSO Services.

Select *Okta* in the list of Services and the pane *SSO Service Details* will appear below the table.

You will need the links note down in the previous section [Configuring Okta to use Awingu as Identity Provider](#).

- **State**: Enable/disable SSO for Okta
- **ACS URL**: the link for *Assertion Consumer Service*
- **Issuer**: the link for *Audience URI*

Adding Okta Applications to Awingu

All applications defined in Okta can be added to Awingu as Web Application. This can be configured in Awingu in System Settings > Manage > Applications:

- **Name**: The application name as it will appear in the Awingu user interface, e.g. Citrix GoToMeeting, Facebook At Work, etc.
- **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. Please use PNG or JPG format.
- **Protocol**: Select *Web Application*.
- **Destination URL**: Enter the *Embed Link* for the Okta application. You can retrieve the link as follows:
 1. As Okta Administrator, login to your Okta account and click on **Admin**.
 2. On the top menu, go to **Applications**.
 3. Click on the desired application.
 4. Click on **General**.
 5. In the section **App Embed Link** you can find the link to use as **Command** in Awingu.

To add a link to Okta Home, you can use base URL of your Okta account.

- **Reverse Proxy**: Disabled.
- **Categories**: Associate zero, one or more application categories to this application.
- **Media Types**: Keep empty: not applicable for web applications.
- **Labels**: Add labels to applications to group them. These groups can be used to filter application servers in lists and reports.
- **Server Labels**: Keep empty: not applicable for web applications.
- **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 [Application Management](#) for more details.

User labels in Awingu only affects whether the application is shown for the user. If the user has valid credentials for the applications configure in Okta, (s)he still will be able to use the application.

Single Sign-On for Salesforce

- [Introduction](#)
- [Linking Salesforce users with AD](#)
- [Setting up Awingu as Identity Provider](#)
- [Configuring Salesforce to use Awingu as Identity Provider](#)
- [Configure Awingu to Enable SSO for Salesforce](#)
- [Adding the Salesforce Application to Awingu](#)
- [Force Salesforce to Use Awingu Only to Sign-In](#)

Introduction

Integrating Single Sign-On (SSO) for Salesforce in Awingu enables following behavior:

- Once signed-in to Awingu, you can open the Salesforce Application directly via Awingu without additional log-in.
- To sign-in to Salesforce, you will be able to select to "Log In Using Awingu", where you can sign-in with your Awingu credentials. Optionally, a you can still choose to be able to sign-in with your Salesforce credentials

Awingu serves as Identity Provider (IdP), as defined in SAML V2.0. This means that Salesforce will check with Awingu if a user is allowed to sign-in to its services.


There is no auto sign-out. Users still need to sign-out from both Awingu and Salesforce separately.


For more in-depth technical information, please refer to [Salesforce's documentation for SSO integration](#).

Linking Salesforce users with AD

In order to configure SSO for Salesforce, you'll need to make sure every user has an Active Directory (or LDAP) account that maps onto a Salesforce account. Awingu uses the e-mail address (*mail* attribute) configured on the AD as account name for Salesforce. In case the e-mail address is not provided, the UPN is used.

The screenshot shows the 'Sam Lovely Properties' window with the 'General' tab selected. The 'E-mail' field is highlighted with a red arrow and contains the value 'sam.lovely@mycompany.com'. The 'First name' field contains 'Sam' and the 'Last name' field contains 'Lovely'. The 'Display name' field contains 'Sam Lovely'. The 'E-mail' field is the primary attribute used for linking Salesforce accounts.

User Detail		Edit	Sharing	Reset Password	Freeze
Name	Sam Lovely				
Alias	saml				
Email	sam.lovely@mycompany.com				
Username	sam.lovely@mycompany.com				
Nickname	SamL 				
Title					
Company					



If you already have your user accounts in your Active Directory, you can sync them with your Salesforce account using **Salesforce Identity Connect**. Detailed instructions can be found [on the Salesforce help pages](#).

Setting up Awingu as Identity Provider

Awingu is configured as IdP via the [User Connector](#) section in the System Settings.

Go to System Settings > Configure > User Connector > SSO Identity Provider (IdP)

- **State:** Enable or Disable IdP functionality in Awingu for all SaaS services.
- **Issuer:** URL from which Awingu is reachable for the end-users, e.g. <https://awingu.mycompany.com/>.
- **Logout URL:** The logout URL redirects the browser to this URL, once the user logs out of the SaaS application that is configured for SSO. By default, the Logout URL is '/' (i.e goes to Awingu main page), but it can hold any valid URL.

SAML V2.0 mandates that responses are cryptographically signed. Awingu uses a certificate and private key to generate the SAML responses. The SaaS service validates the response with the certificate, which should be configured in the service. As there is no certificate authority involved, the certificate can be self signed. Note that the certificate-key pair is the same for all configured SaaS services configured within one Awingu domain.

- **Certificate:** The public X.509 certificate for the provided Issuer in **.crt format/.pem format**, ASCII file, starting with:
-----BEGIN CERTIFICATE-----
- **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-----

The way you generate keys and certificates often depends on your development platform and programming language preference. Here an example is shown how to generate a certificate using [openssl](#) (download for Windows [here](#)) via the command line:

```
set OPENSSL_CONF=C:/OpenSSL-Win32/bin/openssl.cfg
C:\OpenSSL-Win32\bin\openssl.exe genrsa -out private_key.pem 2048
C:\OpenSSL-Win32\bin\openssl.exe req -new -x509 -days 3650 -key
private_key.pem -out certificate.pem
```

When the "Common Name" is asked, please enter your domain name, e.g. [mycompany.com](#).

An alternative way to generate keys: https://www.samltool.com/self_signed_certs.php (note: generating keys via a third party always induces a security risk).

Security Warning

The private key should be kept secret at all times. If this key gets compromised, unauthorized individuals can access to your corporate accounts of the SaaS services.

Configuring Salesforce to use Awingu as Identity Provider

In order to configure Salesforce for SSO, the following steps need to be taken:

1. As Salesforce Administrator, go to **Setup**.
2. Go to **Security Controls > Single Sign-On Settings**.

3. Click on **New**:
<issuer_url> the URL from which the Avingu environment is reachable. E.g. <https://avingu.mycompany.com>
 - a. **Name**: Avingu
 - b. **Issuer**: <issuer_url>. Note the trailing slash, e.g. <https://avingu.mycompany.com/>
 - c. **Identity Provider Certificate**: Upload your your public certificate. This is the same as [provided to Avingu](#).
 - d. **Request Signing Certificate**: Default Certificate
 - e. **Request Signature Method**: RSA-SHA1
 - f. **Assertion Decryption Certificate**: Assertion not encrypted
 - g. **SAML Identity Type**: Assertion contains User's [salesforce.com](#) username
 - h. **SAML Identity Location**: Identity is in the NameIdentifier element of the Subject statement
 - i. **Service Provider Initiated Request Binding**: HTTP POST
 - j. **Identity Provider Login URL**: <issuer_url>/idp/login, e.g. <https://avingu.mycompany.com/idp/login>
 - k. **Identity Provider Logout URL**: <issuer_url>/idp/logout, e.g. <https://avingu.mycompany.com/idp/logout>
 - l. **Custom Error URL**: (empty)
- m. **API Name**: Avingu
- n. **Entity ID**: https://<salesforce_domain>.my.salesforce.com. You can find your <salesforce_domain> in **Domain Management > Domains**.
4. Click on **Save**.
5. Enable **Federated Single Sign-On Using SAML**.
6. In the table with **SAML Single Sign-On Settings**, click on **Avingu**.
 - a. Scroll down to **Endpoints**
 - b. Please note down the **Salesforce Login URL** needed for next section [Adding the Salesforce Application to Avingu](#):

- **Issuer:** You can keep the default value <https://saml.salesforce.com>

Adding the Salesforce Application to Awingu

Salesforce can be added as web application to Awingu in System Settings > Manage > Applications:

- **Name:** The application name as it will appear in the Awingu user interface, e.g. Salesforce.
- **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. Please use PNG or JPG format.
- **Protocol:** Select *Web Application*.
- **Destination URL:** https://<salesforce_domain>.my.salesforce.com. This is the same value you entered for **Entity ID** in the section [Configuring Salesforce to use Awingu as Identity Provider](#).
- **Reverse Proxy:** Disabled.
- **Categories:** Associate zero, one or more application categories to this application.
- **Media Types:** Keep empty: not applicable for web applications.
- **Labels:** Add labels to applications to group them. These groups can be used to filter application servers in lists and reports.
- **Server Labels:** Keep empty: not applicable for web applications.
- **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 [Application Management](#) for more details.

User labels in Awingu only affects whether the application is shown for the user. If the user has valid credentials for Salesforce, (s)he still will be able to use the application.

Force Salesforce to Use Awingu Only to Sign-In

When opening the Salesforce application in Awingu, users will still have the option to choose whether they sign-in via Salesforce directly or via Awingu. To redirect immediately to sign-in via Awingu, you need to configure following on Salesforce:

1. As Salesforce Administrator, go to **Setup**.
2. Go to **Domains > My Domain**.
3. Edit the **Authentication Configuration**:
 - a. Keep Awingu as the only **Authentication Service**.
 - b. Click on **Save**.

You can even go one step further and completely disable direct login to Salesforce:

1. As Salesforce Administrator, go to **Setup**.
2. Go to **Domains > My Domain**.
3. Edit the **My Domain Settings**:
 - a. Enable the **Login Policy**: Prevent login from <https://login.salesforce.com>
 - b. Click on **Save**.

When Awingu is not accessible for the end-user, (s)he won't be able to sign-in to Salesforce if SSO is configured to be required.

Microsoft OneDrive for Business

- Introduction
- Allowing Awingu to access your Office 365 subscription
 - Step 1. Get an Office 365 subscription
 - Step 2. Set up an Azure Active Directory tenant
 - Step 3. Register your app with Azure Active Directory
 - Step 4. Have the network right
- Configuring Awingu to access OneDrive
- Configuring the Awingu OneDrive app
- Using OneDrive on Awingu

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 enoughClick 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

The documentation is quite harsh, but what you actually need to do:

1. Go to <https://portal.azure.com>
2. Go to Azure Active Directory > App registrations
3. Click on Add:
 - a. Name: e.g. "OneDrive on Awingu"
 - b. Application Type: Web app / API
 - c. Home page URL: the URL to your Awingu environment (e.g. <https://awingu.mycompany.com>)
4. Once created, click on the app to retrieve the Client ID = Application ID.
You will need this value to configure Awingu.
5. Click on All settings > Keys and create a key:
 - a. Key description: secret

- b. Expires: never expires
- 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 lose it!

6. Go to Required permissions and click on Add:
 - 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:

- <mydomain>-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
- Awingu 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 All settings > Reply URLs
4. Change the URL to 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).

Microsoft Skype for Business Online

- Introduction
- Allowing Awingu to access your Office 365 subscription
 - Step 1. Get an Office 365 subscription
 - Step 2. Set up an Azure Active Directory tenant
 - Step 3. Register your app with Azure Active Directory
 - Step 4. Have the network right
- Configuring Awingu to access Skype for Business Online
- Using Skype for Business Online in Awingu

Introduction

Users of Skype for Business Online can send the links of shared applications, files and folders to their contacts in Microsoft Skype for Business Online.

We describe in this section how to configure both your Microsoft account and your Awingu environment.

Allowing Awingu to access your Office 365 subscription


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.

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. Go to Azure Active Directory > App registrations
3. Click on Add:
 - a. Name: e.g. "Skype for Business Online on Awingu"
 - b. Application Type: Web app / API
 - c. Home page URL: the URL to your Awingu environment (e.g. <https://awingu.mycompany.com>)
4. Once created, click on the app to retrieve the Client ID = Application ID.
You will need this value to configure Awingu.
5. Click on All settings > Keys and create a key:
 - a. Key description: secret
 - b. Expires: never expires
 - 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 lose it!
6. Go to Reply URLs and add all URLs to your Awingu environment, e.g. https://awingu.mycompany.com/*
7. Go to Required permissions and click on Add:
 - a. Select an API: Skype for Business Online
 - b. Select following delegated permissions:
 - Read/write Skype user contacts and groups
 - Receive conversation invites
 - Read/write Skype user information
 - Create Skype Meetings
 - Initiate conversations and join meetings
 - c. Click on Done

Step 4. Have the network right

Awingu needs to be able to reach the Skype for Business servers directly, or through an HTTP proxy (see [Connectivity Settings](#)). HTTPS (port 443) access is required to:

- *.online.lync.com
- *.infra.lync.com

- login.microsoftonline.com

Configuring Awingu to access Skype for Business Online

Skype for Business Online can be configured for each domain in the System Settings.

1. Go to Configure > User Connector
2. Scroll down to Skype for Business Online Integration and click on the pencil to edit:
 - **State:** Enabled
 - **Client ID:** configured in the previous section
 - **Secret:** configured in the previous section

Using Skype for Business Online in Awingu

When a user wants to send a link to a share for the first time, they will first need to connect to their Office 365 account. This can be done on the Account settings page in Awingu. They will be redirected to the Office login portal where access is requested to his/her Skype for Business Online account. Once access is granted, they can select any of their contacts when sharing a file/folder/session.

Smart Card Redirection

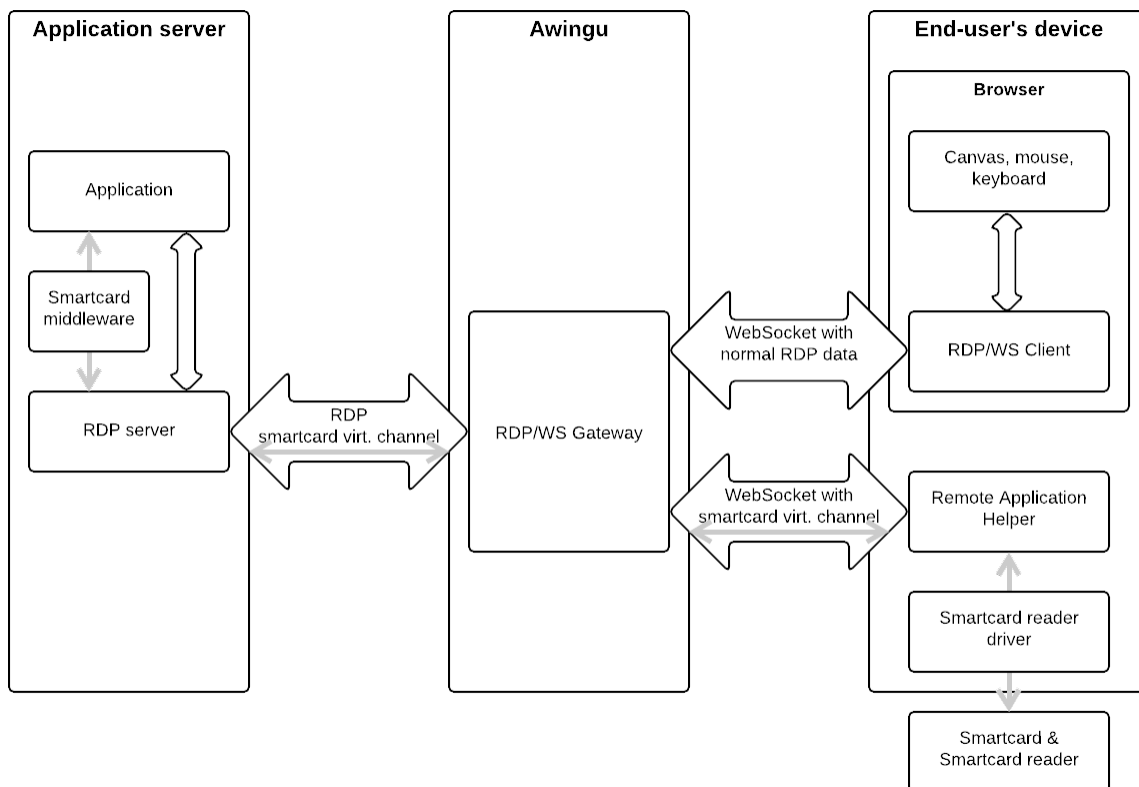
Introduction

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 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*

DEV-AWINGU

Configure

Manage

Changes

Global

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:

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

4.0.0

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, macOS and Linux (tested with Ubuntu 16.04).

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/Linux. Therefore, it might be that some applications on the Windows application server will perform certain library call that is incompatible with the macOS/Linux library available on the end-user device. We have seen this behavior for the eID Viewer and Isabel.

Troubleshooting

- Awingu provides an application called *Browser Check*, available in the user's profile menu. The section "Remote Application Helper" shows whether Awingu is able to connect to it.
If this check is green, but smart cards don't work, please check:
 - whether the driver of the smart card reader is installed on the user's device;
 - 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](#)
 - [PowerShell example using an API Token](#)
 - [Navigating Through the API](#)
 - [Changing Settings](#)
 - [Logging Out](#)
 - [Further documentation](#)
- [Installing with the Awingu API](#)
- [Configuring with the Awingu API](#)

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/](http(s)://your-awingu-environment/api/v2/)
- The API documentation at [http\(s\)://your-awingu-environment/api/v2/docs/](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.

Awingu.com

Manage API token

Close x

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:

Save

Generate new token

Disable token

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 Reset

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

Export CSV

Changes Details

Request

```
{
  "password": "*****"
}
```

Response

```
{
  "token": "*****"
}
```

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

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]::Tls12

$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](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. For more details about the fields that are also shown in the web installer, please refer to [Awingu Installer](#).


```
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"
        },
        "database": {
            "graphite_web": null,
            "frontend_web": null
        },
        "environment": {
            "management_user": {
                "username": "my-admin-user",
                "password": "my-password",
                "confirmed_password": "my-password"
            }
        },
        "appliances": [
            {
                "ip": "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.

Backup and recovery of the Awingu Database

Introduction

The Awingu platform allows to generate a 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 dump and saving it on another system via SFTP. In case of a database or disk failure, you can recover your Awingu environment.

To configure the SFTP user:

1. Go to the System Settings > Global > Connectivity
2. Configure the password for the SFTP user *dbbackup*.

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 want to restore to a fresh new appliance, you will need to "Force" the restore.

If you restored to fresh new appliance, you will need to re-enter following data in System Settings:

- Global > Certificates
- Global > Connectivity > SSL Offloader: SSL mode
- Global > Connectivity > SNMP: Password
- Global > Domains > For each domain: Bind Password
- Per domain: Configure > User Connector > SSO Identity Provider (IdP): Certificate + Private Key
- Per domain: Configure > User Connector > Skype for Business Online Integration: Client ID + Secret
- Per domain: Manage > Drives: Secret for OneDrive backends

It is also recommended to do an *Apply Changes* by modifying the setting Global > Connectivity: Keepalive Disconnected Timeout

Some data are not stored into the database and won't be recovered:

- Insights (in the Dashboard)
- Audit (in the Dashboard)
- Metering data (in the Dashboard)

Note that when opening the Insights after recovery to a **newly installed** appliance, you will be asked to *Configure an index pattern*. Click on create (without changing any settings) to start using the Insights again.