# Set Up Infrastructure Properties

This document describes how to setup the properties of your infrastructure to match the deployment type.



## Overview

Setting up the infrastructure properties is very important. By default, at the VoipNow installation we consider that your infrastructure is going to be provisioned on the public network. While this is appropriate for most single node deployments, it is against the best practices for distributed system deployments.

Therefore, if your infrastructure is using NAT or any private network, it is required to setup the infrastructure properties:

- the first time you install VoipNow
- on upgrade to VoipNow 3.0.0
- before you start provisioning a distributed system

When the Infrastructure Type is changed, **all roles must be reconfigured. This will lead to system downtime!**

## Choose Infrastructure Type

These are the infrastructure types that you can choose from.

### Public IP Cloud

All nodes have public IP addresses only. This setup is appropriate only for small single node deployments.

### Private/Public IP Cloud

All nodes have a private IP address. Nodes that run roles requiring public connectivity also have a public IP address. Many cloud providers deploy their infrastructure in this way, e.g. SoftLayer CloudLayer.

### NAT Cloud

The NAT cloud requires a private network to be defined. All nodes have a private IP address. Nodes that run roles that require public connectivity have a carrier grade NAT layer in front of them, e.g. Amazon Cloud.

## Private Connectivity for VoIP Services

VoIP services require special provisioning information when you have very specific deployment scenarios. In most cases it is not necessary to change these settings!

### Allow private connectivity for VoIP from/to

This setting is available for **NAT Cloud** and **Private/Public IP Cloud** infrastructure types. By enabling it, VoIP services become available in the private network as well (behind NAT). This network or subnetwork must be specified in the available field.

For large deployments it is not typical to enable this option, as you should not have customers in your own private network. But this option might assist you with testing - for example you provision a single node installation in your company network behind NAT and you want to test voice services from the enterprise network, but also from the public network.

### Allow direct routing of VoIP to/from

This option allows the SIP nodes to route traffic to specific networks and to receive traffic from specific networks. It might be necessary when you connect your system to SIP trunks using VPN for additional security and SLA options. When this setting is enabled, it is necessary to define these networks in the **D irect routing network** option.

Multiple networks can be defined, but these require configuration on all SIP and PBX roles as well, therefore treat this option with care!