# 1) A Propos

Ce guide est un des documents décrivant le système de messagerie électronique unifiée de l'Université de Nantes, mis en place depuis septembre 2004. Tout comme le système qu'il documente, ce texte est appelé à évoluer.

Les rédacteurs peuvent être joints à l'adresse électronique suivante : docmessagerie@univ-nantes.fr

Ce document n'est qu'une des différentes éditions disponibles de ce guide. Ces guides sont à l'usage de tout le personnel de l'Université de Nantes. Ces documents se veulent simples et peu techniques. De ce fait de nombreux points de détails sont volontairement laissés sous silence. Du fait de la grande disparité entre le matériel, les systèmes d'exploitation et les habitudes de chacun, plusieurs éditions existent.

Une version plus simple pour la configuration de votre logiciel de messagerie est disponible ici: Configuration de la messagerie

# 2) Tableau de référence

Pour utiliser le système de courrier électronique unifié de l'université, seuls quelques paramètres sont à connaître. Ils sont indiqués dans le tableau suivant, qui servira de référence pour la suite du guide. Bien entendu, seuls les utilisateurs expérimentés peuvent se débrouiller avec ces paramètres. Les chapitres qui suivent permettent d'expliquer pas à pas la configuration complète du système de messagerie, et de clarifier ce tableau.
Dans le tableau suivant, l'exemple d'un utilisateur dont le prénom est **Jean** et le nom de famille **Toto** est considéré.

| **Informations personnelles** | |
|---|---|
| Adresse électronique officielle: | Prenom.Nom@univ-nantes.fr<br>par exemple : **Jean.Toto@univ-nantes.fr** |
| Compte de consultation (login): | <nom>-<1ere lettre du prénom><br>par exemple : **toto-j** |

| **Serveur** | **Adresse** | **Port** | **Infos** |
|---|---|---|---|
| Entrant | **imaps.univ-nantes.fr** | 993 | Le protocole doit être IMAP Sécurisé (ou IMAPS).<br>Les identifiants sont ceux vous ont été fournis lors de votre arrivée (nom-première lettre du prénom) |
| Sortant | **smtp-tls.univ-nantes.fr** | 25 ou 465 ou 587 | Vous devez utiliser le protocole SMTP avec la sécurisation **STARTTLS** ou **TLS** (et pas SSL).<br>Vous devez aussi utiliser les mêmes identifiants que précédemment. |
| Webmail | https://webmail.univ-nantes.fr | - | Pour se connecter facilement de partout avec un simple navigateur web |

**→ Plus d'information sur la configuration de votre client de messagerie: Configuration de votre client de messagerie**

# 2.1) restrictions

Afin de limiter les conséquences des vols d'identifiants, il existe des restrictions concernant l'usage des serveurs de messageries de l'université **lors de l'envoi de courriers électronique**:

- **webmails**:
  - 100 messages par heure
  - 500 destinataires par quart d'heure (les tentatives étant comptabilisées)
  - 1000 destinataires par heure (les tentatives étant comptabilisées)
- **smtp(-tls).univ-nantes.fr**
  - utilisation de l'intérieur de l'université:
    - 100 messages par heure
    - 500 destinataires par quart d'heure (les tentatives étant comptabilisées)
    - 1000 destinataires par heure (les tentatives étant comptabilisées)
  - utilisation de l'extérieur de l'université:
    - 50 messages par heure
    - 500 destinataires par quart d'heure (les tentatives étant comptabilisées)
    - 1000 destinataires par heure (les tentatives étant comptabilisées)
- **smtp.univ-nantes.prive**
  - 100 messages par heure

# 3) Objectifs

Changer de système de courrier électronique n'est pas un processus anodin. De nombreuses justifications sur ce processus sont consultables dans le guide avancé. En quelques mots, l'Université de Nantes disposait de plus de cinquante serveurs de courriers électroniques, avec une grande disparité sur les moyens techniques et humains engagés, sur le nombre d'utilisateurs, sur la qualité du service fourni. Certains de ces serveurs étaient en bon état, d'autres ont montré de nombreux problèmes (sécurité, virus, spam, pannes). Dans un but d'homogénéiser ce processus, il a été décidé d'unifier la totalité de la messagerie électronique en un service unique, de façon à apporter :

- Homogénéité (Tous les courriers électroniques sont de la forme Prenom.Nom@univ-nantes.fr), avec possibilité de conserver les anciennes adresses. Il est également possible de créer des alias et des adresses fonctionnelles (Directeur.Composante@univ-nantes.fr, par exemple).
- Sécurité : une plus grande disponibilité des serveurs, des sauvegardes régulières, des systèmes de redondance pour éviter la perte de messages. Cela, grâce à des serveurs dédiés, sécurisés et sauvegardés. Des permanences seront assurées pendant les vacances.
- Égalité : tous les personnels disposent de la même qualité de service, quel que soit son service ou son UFR de rattachement. Tous les utilisateurs disposent donc des mêmes fonctions avancées, comme l'antivirus et l'anti SPAM, ainsi qu'un webmail efficace.
- Simplicité : toutes les machines seront configurées de la même façon. Des services d'accès à distance sont disponibles. Tout nouvel arrivant à l'université reçoit automatiquement une adresse électronique.
- Evolutivité : le système est conçu pour pouvoir évoluer continuellement et bénéficier des dernières nouveautés technologiques, et ce, de la façon la plus douce possible pour l'utilisateur.

Des plate-formes de tests sont disponibles pour l'équipe technique, afin de tester et valider en permanence les nouvelles technologies, notamment celles qui sont actuellement en évolution rapide (lutte anti-spam, par exemple).

# 4) Rappels sur la messagerie, et application pour l'université de Nantes.

L'outil de messagerie est utilisé par tout le monde à l'université, et de ce fait, est un outil relativement bien connu. Malgré tout, peu de personnes sont capables de régler leur logiciel de messagerie eux-mêmes. Pourtant, les informations à connaître pour configurer correctement son logiciel sont peu nombreuses (cf tableau, page 6). La difficulté réside dans la connaissance de l'utilité de chacun de ces paramètres. Les quelques informations ci-dessous devraient rendre la chose plus aisée.

En simplifiant, et d'une manière générale, le circuit d'un message est le suivant : une personne, l'expéditeur, rédige un message à destination d'une autre personne : le récepteur. Le message est envoyé du poste local vers le serveur de messagerie. Le message électronique emprunte alors le réseau, pour être ensuite stocké dans la boîte aux lettres du destinataire. Celle-ci est ensuite consultée par le récepteur, grâce à un logiciel de messagerie. Il lit ce message, puis décide ou non d'y répondre. Et le circuit recommence. Chaque étape va maintenant être détaillée.

## La réception d'un message

Lorsqu'un message arrive pour l'université, les points suivants sont vérifiés :

- Il est à destination d'une adresse électronique valide. (L'annuaire des personnels de l'université est consulté)
- Une première analyse est effectuée pour détecter une présence éventuelle de virus.

Si les points 1 et 2 sont remplis, le message est accepté. Sinon, il est rejeté.

- Ensuite, une seconde analyse du message est effectuée pour évaluer la probabilité qu'il s'agisse d'une publicité ou d'un publi-postage non sollicité. (Communément appelé SPAM) -voir la rubrique SPAM-. Si cette probabilité est importante, alors le titre du message est préfixé par [SPAM]. Voir la rubrique SPAM pour plus d'informations.
- Le message est alors délivré dans la boîte aux lettres du destinataire.

## Consultation du compte de messagerie.

Il est souvent question de compte de messagerie, par analogie au compte bancaire. Le compte de messagerie est un espace qui vous est personnel, protégé par un secret (le mot de passe), dans lequel vous pouvez retirer des messages, et grâce auquel vous pouvez aussi envoyer ou transférer des messages. Le compte de messagerie englobe votre boîte à lettres, et la façon dont vous devez y accéder.

# Authentification

Pour consulter sa boîte aux lettres (accéder à son compte), il est donc nécessaire de s'identifier. Chaque personnel de l'université dispose d'un identifiant unique avec son mot de passe. Cet identifiant est du format <nom>-<1ère lettre du prénom> (voir tableau page 6 ) : par exemple : toto-j pour Mr Jean Toto. C'est le login. Il est unique, et référencé dans l'annuaire de l'université, appelé annuaire DYNA, auquel vous pouvez accéder sur http://dyna2.cri.univ-nantes.fr

Si votre prénom est composé, le login prend les initiales de deux prénoms, exemple : Jean-Pierre Toto ⇒ toto-jp. En cas de collision avec le login d'une personne précédemment saisie dans la base de données, on ajoute un chiffre à la fin du login. Exemple (sachant que Jean Toto existe déjà) : Jérôme Toto ⇒ toto-j-1. Une centaine de personnes sont concernées, parmi le personnel de l'université.

Votre login est associé à un mot de passe, permettant au système d'information de s'assurer que vous êtes bien la personne que vous prétendez être. Les mots de passe sont sensibles aux différences entre MAJUSCULES et minuscules. Attention lorsqu'ils sont tapés au clavier. Les mots de passe devront obligatoirement être changés tous les six mois, pour des raisons de sécurité.

Votre login, ainsi que votre mot de passe initial, vous ont été communiqués par écrit ou via l'ancien système de messagerie, par un correspondant du CRI au niveau de votre composante de l'université. Celui-ci est habilité à renouveler votre mot de passe, si vous l'oubliez.

# Changement de mot de passe

Pour changer votre mot de passe, connectez-vous avec un navigateur récent (Microsoft Internet Explorer, Mozilla ou FireFox) depuis le réseau de l'université sur :

- https://motdepasse.univ-nantes.fr

Dans la rubrique en haut à droite « Connexion à Dyna », entrez vos identifiants de connexion fournis par la DSI, puis cliquez sur « OK ». Votre mot de passe sera chiffré sur le réseau, entre votre ordinateur et le serveur de la DSI. Sur la page suivante, cliquez en haut à droite sur « Changer le mot de passe » et remplissez alors les informations demandées. Le mot de passe que vous choisirez devra être de bonne qualité afin de pas pouvoir être deviné par quelqu'un d'autre, autrement il sera refusé par le serveur. Vous ne devez le communiquer à personne.

# Consultation des messages dans les boîtes aux lettres

Le logiciel de messagerie, installé sur les postes clients (Thunderbird) peut alors consulter la boîte aux lettres de l'utilisateur. La méthode de choix est le protocole IMAP:

Ce protocole est plus récent et également plus avancé. Il diffère de POP dans le fait que les messages sont conservés sur le serveur, et qu'il est possible d'y créer des dossiers personnels. Le fait que les messages soient laissés sur le serveur implique une surveillance de la place disque occupée (voir la rubrique QUOTAS pour plus d'informations). le serveur est :

```
imaps.univ-nantes.fr
```

## Envoi de messages

Dans le système de courrier électronique de l'université, le flux de réception des messages a été séparé de celui de l'envoi. L'envoi de message se fait par le protocole standard, SMTP. Le serveur est :

```
smtp-tls.univ-nantes.fr
```

Il faut aussi préciser la sécurisation STARTTLS (ou TLS) et utiliser l'authentification simple avec vos identifiants

## Identification à l'extérieur

Il est rappelé que l'adresse officielle est Prenom.Nom@univ-nantes.fr.

L'ancienne adresse (avec un suffixe contenant le nom de l'UFR, du laboratoire ou du service) est conservée en tant qu'alias, afin de ne pas perdre des messages à destination d'une adresse électronique bien connue ou diffusée par le passé. Cependant, il n'est pas conseillé de l'utiliser de façon officielle.

# 5) Fonctions avancées et changements par rapport à l'ancien système

La mise en place d'un système de courrier électronique à l'échelle de l'université ne se conçoit pas de la même façon qu'un système de courrier électronique pour une petite équipe. Des choix techniques et politiques sont faits. Ce chapitre explique rapidement les particularités du système.

## Anti Spam

Le SPAM fait référence aux « courriers non sollicités », c'est à dire des courriers de publicité, envoyés en très grand nombre. Le nombre de SPAM en circulation est en constante augmentation depuis quelques années, au point de représenter plus de 80% du trafic mondial. Il est absolument nécessaire de combattre ce fléau qui fait perdre beaucoup de temps à tout le monde.

Le système mis en place fonctionne sur deux principes :

- Inspection de l'aspect du message (sa forme). Dans cette passe, le système vérifie l'intégrité du message et cherche des indices souvent employés lors d'émission de spams (code html intégré au corps du message, liens à cliquer, en-têtes tronqués ou faussés, etc…)
- Confrontation du message avec système à apprentissage. Dans cette passe le contenu du

message est confronté à une base de données d'information sur les messages connus comme spam. Si le message reçu ressemble à de précédents messages reçus et classifiés comme spam, alors il y a de grandes chances que ce nouveau message en soit lui aussi. Cette base peut être éduquée en corrigeant ses erreurs de diagnostics. Seuls les gestionnaires du système de courrier électronique peuvent faire cette manipulation.

Chacune de ces deux passes donne un score, supérieur à 0 si le message semble être correct, < 0 si le message semble être du SPAM. Un score global est calculé, et si le score global est < 0, le message est considéré comme étant probablement un SPAM. Il est alors étiqueté comme tel (préfixe [SPAM] dans le sujet du message). Dans tous les cas, le message est délivré.

**Il n'y a pas de suppression, effacement, ou modification du contenu du message.**

→ **Plus d'information sur le SPAM à l'Université de Nantes: Documentation Spam**

### Limitations du système.

Le système anti spam (comme tout système de ce type), **ne peut être fiable à 100%**. A ce titre, il est purement indicatif, et il ne faut pas lui donner une confiance trop forte. Il peut arriver que des messages tout à fait valides soient étiquetés comme SPAM. La lutte anti SPAM étant actuellement un point de recherche important en informatique, le système de messagerie de l'université va évoluer en permanence pour appliquer au mieux les dernières technologies de lutte.

Si des messages sont faussement étiquetés [SPAM], il faut les faire suivre, en pièces jointe, à:

```
traitementspam@univ-nantes.fr
```

Il est important que le message original ne soit pas altéré, c'est pour cela que le transfert en tant que pièce jointe est la seule façon de faire. Certains logiciels (Eudora et Outlook par exemple) ne sont malheureusement pas capables de le faire correctement.

Dans le cas de versions récentes d' Eudora, il est possible de contourner le problème en sauvant le message initial sur le disque, puis de l'envoyer en tant que pièce jointe. Si des filtres automatiques redirigent automatiquement les messages étiquetés [SPAM] dans un dossier, il est vivement recommandé de vérifier périodiquement le contenu de ce dossier afin d'y détecter d'éventuels messages faussement étiquetés. Il serait extrêmement dangereux de supprimer le contenu de ce dossier avant de faire une vérification rapide.

→ **Plus d'information sur la correction antispam: Corriger l'antispam**

## Anti Virus

Deux anti-virus différents (McAfee Viruscan et Clamav) testent tous les messages qui entrent dans l'université, ainsi que tous ceux qui sortent. Les messages contaminés sont mis en quarantaine. Les mises à jour de ces anti virus se font plusieurs fois par jour.

Néanmoins, les postes clients Windows doivent **TOUJOURS** être protégés eux-mêmes par un anti virus local et à jour. En effet, la messagerie n'est pas l'unique vecteur de contamination des virus

informatiques.

Conformément aux avis du CERT français, (organisme gérant la sécurité des réseaux), nous n'indiquons ni aux envoyeurs, ni aux récepteurs, le fait qu'un virus ait été stoppé. En effet, les virus modernes maquillent les adresses d'expéditeurs et de destinataires. Prévenir le supposé expéditeur que son message contient un virus ne marche quasiment jamais. Cela a, en général, pour effet de remplir une boîte aux lettres d'un innocent et de générer une surcharge au niveau du réseau et des serveurs.

**→ Plus d'information sur la politique antivirale de la messagerie de l'Université de Nantes: La protection antivirale**

# Quotas

Pour éviter un engorgement de l'espace de stockage, qui est commun à tous les personnels de l'université, il est nécessaire de mettre en place des quotas. Il s'agit d'une limite quant à l'espace de stockage que chaque utilisateur a le droit d'utiliser. Suivant le profil de l'utilisateur, les limites sont les suivantes :

## Quotas de la boîte de réception

| **Profil type de l'utilisateur** | **Quota** |
|---|---|
| Chercheur invité, vacataire | 1Go |
| Utilisateur type | 1Go |
| Directeur de composante, demandes explicites | + de 1Go suivant besoins |

## Quotas de taille maximum de message.

Pour tous les utilisateurs, la limite est de 20 Mo. Si des documents d'une taille supérieure doivent être échangés, ils doivent l'être par des méthodes plus adéquates (FTP, serveur WEB, messagerie instantanée de l'université). Échanger des documents d'une telle taille par le courrier électronique est inadapté.

## Gestion efficace de son quota

L'espace de stockage est limité sur les serveurs. Il est suffisant dans le cadre d'une utilisation normale du service. Néanmoins, pour éviter tout éventuel débordement, quelques précautions sont à prendre.

L'idée est de ne garder que les messages importants sur le serveur. Les personnes abonnées à des listes de diffusion trient, en général, leurs messages automatiquement, grâce à des filtres automatiques (voir plus loin). Ces filtres déplacent automatiquement les messages dans un sous-dossier de messagerie. Ces sous-dossiers peuvent être stockés soit sur la machine locale, soit sur le serveur (si IMAP est utilisé). Les sous-dossiers stockés sur le serveur sont comptabilisés dans le quota.

### Suppression des messages

La suppression d'un message sur le serveur l'envoie dans la poubelle. Il est important de savoir que tant que la corbeille n'a pas été vidée, le message est toujours présent et donc comptabilisé dans le quota. Il est donc important de vider périodiquement la corbeille de messagerie.

### Ne pas garder de messages inutiles sur le serveur

Il est facile de sélectionner les messages ayant au moins trois mois dans sa boîte et de les archiver dans un sous-dossier. Il est conseillé de les archiver en local.

## Protocoles sécurisés POPS, IMAPS

POPS et IMAPS sont les versions sécurisées des protocoles pop et imap, déjà détaillés auparavant. Ces versions sont obligatoirement à utiliser si le compte de messagerie doit être accédé depuis l'extérieur. En effet, l'utilisation des protocoles POP et IMAP implique que les mots de passe de l'utilisateur transitent sur l'Internet de façon non sécurisée. Ce qui peut s'avérer dangereux lorsque la communication s'effectue via un réseau tiers (Fournisseur d'accès Internet, réseau étranger...).

Pour cette raison, l'accès aux protocoles POP et IMAP est désactivé à l'extérieur de l'université.

POPS est désactivé à l'extérieur de l'université car il s'accorde assez mal avec l'utilisation du webmail ; en outre, il nécessite une connexion nettement plus rapide qu'IMAPS, ce qui n'est pas garanti à l'extérieur de l'université.

## Filtrages

Un message électronique est constitué de deux parties, par analogie avec le courrier papier : l'enveloppe du message et le corps du message. Une enveloppe papier contient essentiellement l'adresse du destinataire et l'horodatage. La version électronique contient aussi l'expéditeur et tout un tas d'informations utiles (par exemple, le fait que le message soit envoyé par une liste de diffusion). Un filtre électronique peut examiner sur l'un ou l'autre de ces éléments et déplacer automatiquement les messages dans un sous dossier.

**→ Plus d'information sur l'utilisation des filtres (par exemple pour trier les spams): Documentation "Filtre"**

## La sauvegarde de la messagerie

La messagerie est sauvegardée régulièrement, en principe chaque jour, de manière automatisée. Sont sauvegardés à la fois les systèmes, c'est-à-dire tous les programmes qui entrent en oeuvre pour faire fonctionner la messagerie et également les données des utilisateurs.

A quoi servent ces sauvegardes ? A restaurer les systèmes et les données en cas de sinistre (pannes matérielles sur un serveur, problèmes logiciels lors d'une mise à jour des systèmes par exemple, etc…).

Ces sauvegardes permettent aussi de restaurer les messages des usagers. Il faut savoir que les données ne sont sauvegardées qu'une fois par jour. En fait, chaque nuit, une photographie des boîtes à lettres est réalisée et sauvegardée sur bandes magnétiques. Avec ce principe, un message arrivé en journée et détruit par son destinataire le jour même, n'est pas sauvegardé, puisqu'il n'existe plus au moment de la sauvegarde qui a lieu la nuit.

Il faut absolument utiliser le protocole IMAP ou IMAPS pour pouvoir bénéficier de ce service de restauration. Le protocole POP ne conserve pas, en général, les messages sur le serveur.

Les sauvegardes des 30 derniers jours (voire quelques jours en plus) sont conservées sur bandes. Au-delà, rien n'est gardé.

# Redirection automatique des messages

Le courrier électronique étant le moyen de communication officiel de l'Université de Nantes, il est nécessaire de pouvoir garantir que tout message envoyé à une adresse universitaire sera bien délivré sur le compte de l'utilisateur. Si le message ne peut être livré, l'université doit pouvoir le justifier: virus, quota plein, etc.

Si l'utilisateur demande une redirection de sa messagerie vers une autre adresse, l'université doit être en mesure de pouvoir faire confiance au gestionnaire de la nouvelle adresse de destination. C'est pour cela que seules les adresses professionnelles sont acceptées dans une redirection. Il n'est pas possible de garantir qu'un courrier envoyé à un service de messagerie personnelle gratuite comme hotmail, yahoo, gmail, free, orange, etc. sera bien livré à son destinataire. De plus en cas de soucis, il est très difficile voire impossible d'obtenir une raison de la part de ces services gérants des millions d'adresses.

L'utilisateur doit demander au service informatique de sa composante pour obtenir une redirection.

### Cas acceptés

- L'utilisateur est un chercheur d'un laboratoire partenaire de l'université: inserm, chu, in2p3, subatech, cnrs, etc, il peut demander à recevoir sa messagerie univ-nantes.fr sur la boîte de son laboratoire.
- L'utilisateur est un chercheur étranger dans une structure de recherche étrangère en déplacement ou détachement à l'université. Il peut demander à recevoir sa messagerie dans sa boîte professionnelle étrangère.

→ **Plus d'information sur la relève d'une messagerie extérieure: Proxy POP/IMAP**

### Cas refusés

- L'utilisateur désire utiliser sa boite personnelle pour communiquer professionnellement.

# 6) Régler son ordinateur.

Pour accéder au système de messagerie unifiée, il faut :

- (Re)-régler son logiciel de messagerie.
- Éventuellement, suivant les sites, procéder à quelques réglages additionnels de l'ordinateur. Ce point n'est abordé que dans certaines éditions de ce document (dans les éditions « sites » concernées).

## Paramétrer son logiciel de messagerie.

Régler son logiciel consiste à remplir des boîtes de dialogue avec les informations données précédemment dans le tableau page 6. Globalement, tous les logiciels récents se configurent de la même façon. Les logiciels de messagerie les plus répandus dans l'université sont passés en revue. Ce chapitre est dépendant de l'édition de ce document (celui ci est l'édition Lina), et donc, plus ou moins long.

Cette édition documente tous les logiciels de messagerie les plus répandus à l'université.

Tous les exemples qui suivent (quel que soit le logiciel documenté) seront pris pour une personne dont le prénom est Jean, et le nom de famille est Toto. Son adresse électronique officielle est donc Jean.Toto@univ-nantes.fr. Dans les exemples, le protocole IMAP est choisi lorsqu'il est proposé.

→ **Plus d'information sur la configuration de votre client de messagerie: Configuration de votre client de messagerie**

## Webmail (Squirrelmail)

Squirrelmail est le nouveau webmail de l'université. Plus rapide et plus puissant que son prédécesseur (NOCC), il offre une prise en main rapide. Il suffit d'un navigateur web pour y accéder.

Le webmail est disponible à l'adresse suivante:

- https://webmail.univ-nantes.fr

→ **La documentation détaillée du webmail est disponible ici: Documentation Webmail**