HCL – 2024

HCL Domino
Certificate of Completion
DOMINO V12: TIME-BASED ONE-TIME PASSWORD (TOTP) AUTHENTICATION
Vincent Gicquel
FOR DEMONSTRATING COMPETENCE AND UNDERSTANDING OF THE MATERIALS AND SUCCESSFUL COMPLETION OF ALL COURSE REQUIREMENTS.
CERTIFICATE
HCLSoftware
OF COMPLETION
Jan 23, 2024
DATE ISSUED
HCLSoftware U
Tiffany Amos
SIGNATURE

HCL Domino

Certificate of Completion

HDOM-ADM-101: INSTALL & CONFIGURE A DOMINO NETWORK

Vincent Gicquel

FOR DEMONSTRATING COMPETENCE AND UNDERSTANDING OF THE MATERIALS AND SUCCESSFUL COMPLETION OF ALL COURSE REQUIREMENTS.

Dec 14, 2023
DATE ISSUED

HCLSoftware U

Tiffany Amos
SIGNATURE

HCL Domino

Certificate of Completion

HDOM-ADM-102: ADMINISTRATION BASICS

Vincent Gicquel

FOR DEMONSTRATING COMPETENCE AND UNDERSTANDING OF THE MATERIALS AND SUCCESSFUL COMPLETION OF ALL COURSE REQUIREMENTS.

Feb 28, 2024
DATE ISSUED

HCLSoftware U

Tiffany Amos
SIGNATURE

HCL Domino

Certificate of Completion

HDOM-ADM-103: DOMINO SECURITY

Vincent Gicquel

FOR DEMONSTRATING COMPETENCE AND UNDERSTANDING OF THE MATERIALS AND SUCCESSFUL COMPLETION OF ALL COURSE REQUIREMENTS.

Feb 28, 2024
DATE ISSUED

HCLSoftware U

Tiffany Amos
SIGNATURE

Android Enterprise – 2023

[Android Enterprise Certified Professional]

[Android Enterprise Certified Associate]

IBM – 2023

MobileIron – Ivanti – 2023

in-zta

in-ztafe

neurons-mdm-support-specialist-2023

epm-administration-2023

epmm-fundamentals-2023

epmm-support-specialist-2023

HCL Connections Docs : Watermak

Comment ajouter un « Watermark » ou un filigrane sur vos documents dans HCL Connections.

Il faut vérifier que HCL Connections Docs soit bien installé sur votre plateforme HCL Connections. Pour se faire ouvrez un navigateur à l'url suivante https://**urlconnections**/docs/version

urlconnections étant l’url de votre HCL Connections

Voici ce que vous devez obtenir :

{"build_description":"HCL Connections Docs 2.0.2","product_name":"HCL Connections Docs","version":"2.0.2","build_timestamp":"20220819-1124"}

Si votre version est supérieure à 2.0 CR2 iFix003, vous pouvez configurer cette option.

Après cette vérification, vous pouvez activer l’option de « Watermak » ou filigrane sur vos documents word, excel etc..

Voici les étapes :

1. Arrêter le serveur Viewer
2. Se déplacer dans le répertoire suivant
   - Pour linux : /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/config/cells/docsCell01/IBMDocs-config
   - Pour Windows : S:\HCL\WebSphere\profiles\Dmgr01\config\cells\Cell01\IBMDocs-config (à adapter selon son installation)
3. Editer le fichier **viewer-config.json**
4. Dans la partie **HtmlViewerConfig**, chercher le paramètre **Watermark**

```
"Watermark":
     {
          "enabled": "true",
          "text_watermark":
          {
               "text":"CONFIDENTIAL CompanyName",
               "font":"Arial",
```

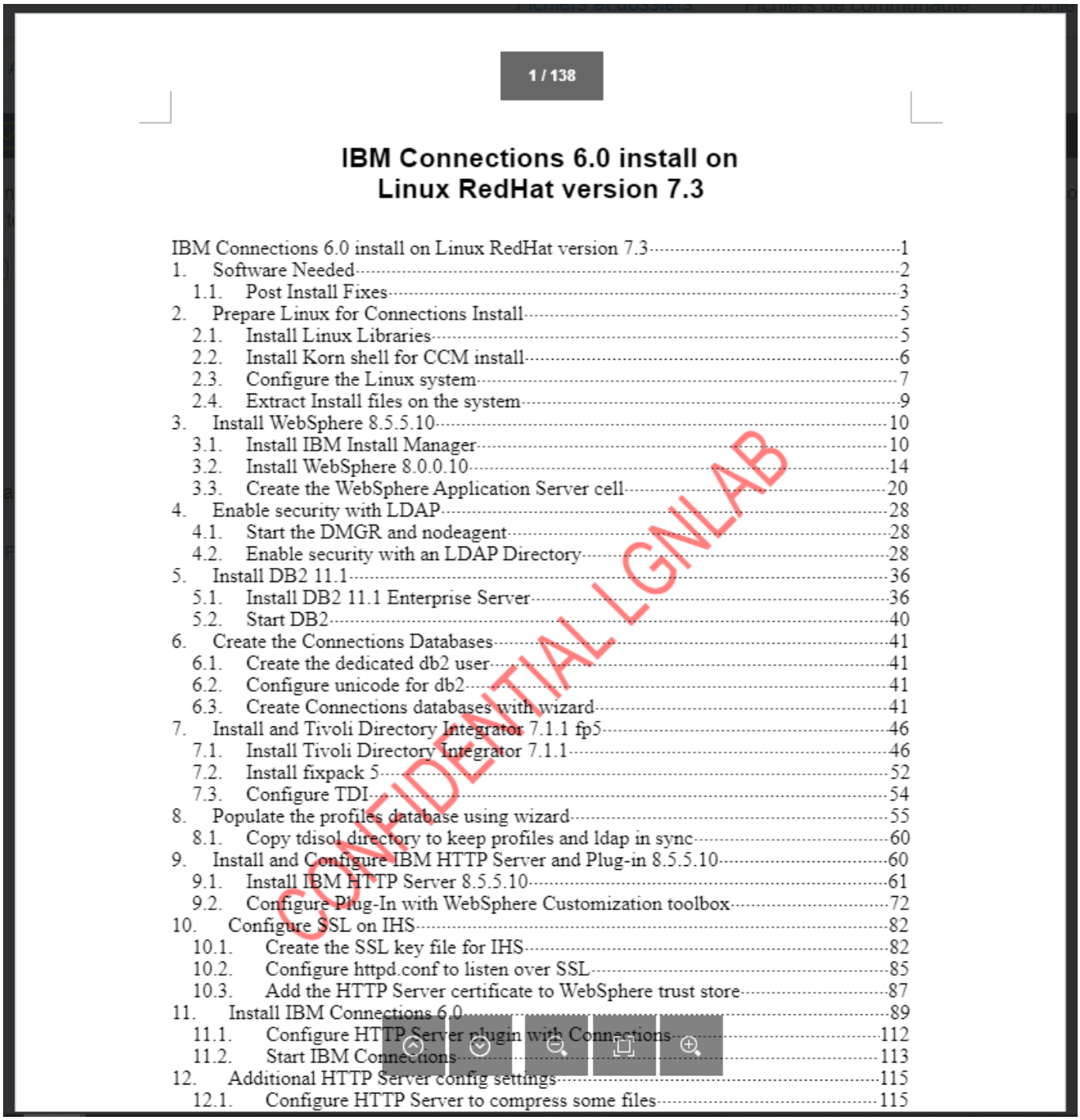
```
                                    "size":"72",
                                    "color":"#D2D2D2",
                                    "diagonal": "true"
                            }
                    }
```

5. Vérifier que le paramètre « enabled » soit à **true**
6. Dans la partie « text_watermark », on peux modifier les différents paramètres :
    - text est le texte que vous souhaitez voir afficher
    - font est la police de caractère du texte
    - size est la taille du texte
    - color est la couleur du texte en hexadécimal
    - diagonal est le paramètre si vous souhaitez voir le texte en diagonale, si vous mettez false, il sera affiché en horizontal
7. Effectuer une synchronisation totale
    - Se connecter à la console d'administration Websphere
    - Cliquer sur **System administration** -> **Nodes**
    - Sélectionner **Nodes01**
    - Cliquer sur **Full Resychronize**
    - Cliquer sur **System administration** -> **Node agents**
    - Sélectionner **nodeagent**
    - Cliquer sur **Restart**
8. Redémarrer le serveur Viewer

Voici un exemple de filigrane :

```
        "Watermark":
                {
                        "enabled": "true",
                        "text_watermark":
                        {
                                "text":"CONFIDENTIAL LGNLAB",
                                "font":"Arial",
                                "size":"36",
                                "color":"#FF0000",
```

```
                "diagonal": "true"
            }
        }
```



1 / 138

IBM Connections 6.0 install on Linux RedHat version 7.3

IBM Connections 6.0 install on Linux RedHat version 7.3 1
1. Software Needed 2
1.1. Post Install Fixes 3
2. Prepare Linux for Connections Install 5
2.1. Install Linux Libraries 5
2.2. Install Korn shell for CCM install 6
2.3. Configure the Linux system 7
2.4. Extract Install files on the system 9
3. Install WebSphere 8.5.5.10 10
3.1. Install IBM Install Manager 10
3.2. Install WebSphere 8.0.0.10 14
3.3. Create the WebSphere Application Server cell 20
4. Enable security with LDAP 28
4.1. Start the DMGR and nodeagent 28
4.2. Enable security with an LDAP Directory 28
5. Install DB2 11.1 36
5.1. Install DB2 11.1 Enterprise Server 36
5.2. Start DB2 40
6. Create the Connections Databases 41
6.1. Create the dedicated db2 user 41
6.2. Configure unicode for db2 41
6.3. Create Connections databases with wizard 41
7. Install and Tivoli Directory Integrator 7.1.1 fp5 46
7.1. Install Tivoli Directory Integrator 7.1.1 46
7.2. Install fixpack 5 52
7.3. Configure TDI 54
8. Populate the profiles database using wizard 55
8.1. Copy tdisol directory to keep profiles and ldap in sync 60
9. Install and Configure IBM HTTP Server and Plug-in 8.5.5.10 60
9.1. Install IBM HTTP Server 8.5.5.10 61
9.2. Configure Plug-In with WebSphere Customization toolbox 72
10. Configure SSL on IHS 82
10.1. Create the SSL key file for IHS 82
10.2. Configure httpd.conf to listen over SSL 85
10.3. Add the HTTP Server certificate to WebSphere trust store 87
11. Install IBM Connections 6.0 89
11.1. Configure HTTP Server plugin with Connections 112
11.2. Start IBM Connections 113
12. Additional HTTP Server config settings 115
12.1. Configure HTTP Server to compress some files 115

CONFIDENTIAL LGNLAB

Comment connaître la version de HCL Connections Docs installée

Pour connaître la version de HCL Connections Docs installée, nous avons plusieurs moyens d'obtenir l'information nécessaire :

Il faut aller voir dans le fichier systemOut.log du serveur Docs, trouver la ligne suivante et noter le numéro d'ifix_version :

IBMDocs build info:{"ifix_version":**34**,"build_version":"2.0.0","build_description":"HCL Connections Docs 2.0.0","product_name":"HCL Connections Docs","build_timestamp":"20200420-1929","patch_base_build":"IBMConnectionsDocs_2.0.0_20151209-1532"}

On peux aussi aller sur la page web suivante https://url_connections/docs/version et récupérer le numéro de l'ifix

{"ifix_version":**34**,"build_description":"HCL Connections Docs 2.0.0","product_name":"HCL Connections Docs","version":"2.0.0","build_timestamp":"20200420-1929","patch_base_build":"IBMConnectionsDocs_2.0.0_20151209-1532"}

Avec le numéro de l'ifix, nous allons le croiser avec le tableau ci-dessous pour obtenir la version de HCL Connections Docs installée.

Docs 2.0 iFix 003	**3**
Docs 2.0 iFix 004	4
Docs 2.0 iFix 005	5
Docs 2.0 CR1	6
Docs 2.0 CR1 iFix 001	7
Docs 2.0 CR1 iFix 002	8
Docs 2.0 CR1 iFix 003	9
Docs 2.0 CR2	15
Docs 2.0 CR2 iFix 001	16
Docs 2.0 CR2 iFix 002	17
Docs 2.0 CR2 iFix 003	18
Docs 2.0 CR2 iFix 004	19
Docs 2.0 CR3	25
Docs 2.0 CR3 iFix 001	26
Docs 2.0 CR3 iFix 002	27
Docs 2.0 CR3 iFix 003	28
Docs 2.0 CR3 iFix 004	29
Docs 2.0 CR3 iFix 005	30
Docs 2.0 CR3 iFix 006	31
Docs 2.0 CR3 iFix 007	32
Docs 2.0 CR3 iFix 008	33
Docs 2.0 CR3 iFix 009	34

Si vous n’avez pas l’information « ifix_version » lors de l’accès à la page suivante https://url_connections/docs/version, il suffit de regarder l’information « version » et dans notre cas, nous sommes en verson 2.0.2 (1) :

{"build_description":"HCL Connections Docs 2.0.2","product_name":"HCL Connections

Docs","**version":"2.0.2**","build_timestamp":"20220819-1124"}

(1) – Pour les versions 2.0.1 et 2.0.2, il n'y a pas de paramètres ifix_version.

HCL Domino 12 : DKIM

Avec la version 12 de Domino, nous pouvons utiliser DKIM (DomainKeys Identified Mail) pour signer les messages envoyés par les utilisateurs internes vers des domaines internet externes. Nous allons dans cet article décrire brièvement ce que le DKIM, comment il fonctionne et comment le configurer sur un serveur HCL Domino 12.0.2.

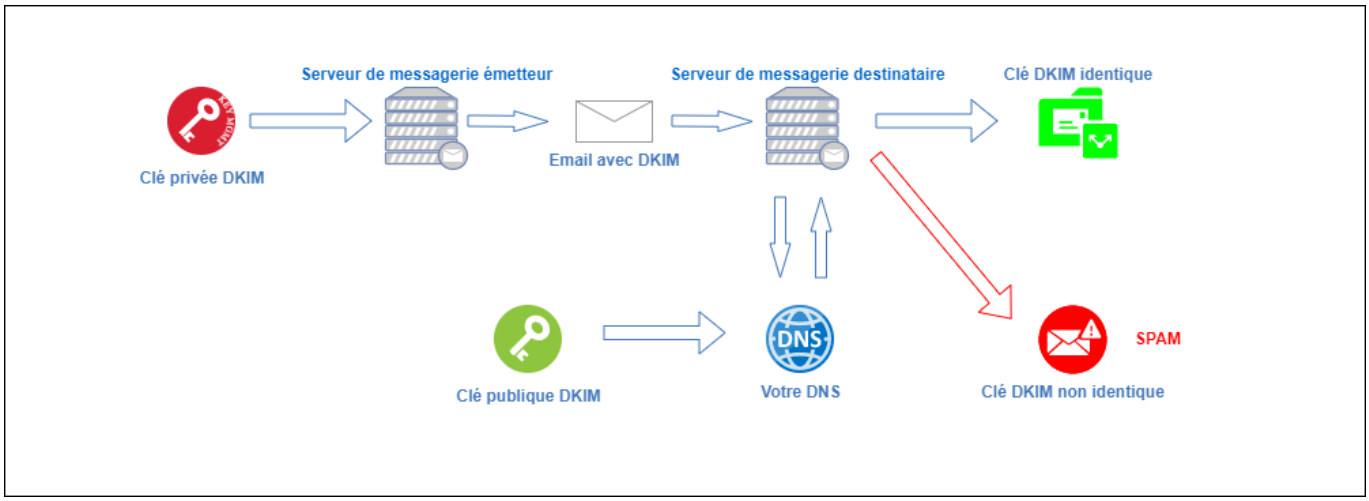
Le DKIM, qu'est ce que c'est ?

C'est une méthode d'authentification qui permet d'éviter l'usurpation d'adresses électroniques, renforce la sécurité du courrier électronique en permettant au serveur de messagerie du destinataire de vérifier l'authenticité du domaine de l'expéditeur.

Comment le DKIM fonctionne t il ?

Le concept de DKIM fonctionne avec deux clés DKIM. La clé publique de l'enregistrement DNS pour vérifier l'authenticité du message par le serveur destinataire et la clé privée pour votre serveur de messagerie dans le cadre de l'authentification.

- Envoi d'un message avec un en-tête DKIM généré par une clé privée
- Vérification de l'authenticité du DKIM de l'expéditeur
- A la réception du message par le serveur destinataire, vérification de la signature DKIM grâce à la clé publique se trouvant dans l'enregistrement DNS de l'expéditeur
- Si la clé publique correspond à la signature DKIM, le message est distribué
- Si la clé publique ne correspond pas à la signature DKIM, il est fort probable que le message soit envoyé dans les spams ou bloqué par l'antispam



DKIM et Domino

DKIM est disponible pour les serveurs Domino depuis la version 12 que ca soit sur Linux ou Windows. Voici les différentes étapes à suivre pour configurer DKIM sur votre serveur Domino.

- Création des clés de signature DKIM dans le magasin de données d'identification.
- Création d'un enregistrement TXT DNS contenant la clé et ajoutez-le à vos paramètres de domaine DNS.
- Spécification de la clé à utiliser pour la signature

DKIM (via notes.ini) sur le serveur.
- Activation de la signature DKIM (via notes.ini) sur le serveur.

Création des clés de signature DKIM

keymgmt create DKIM *domain selector* RSA [*keySize*]

Avec

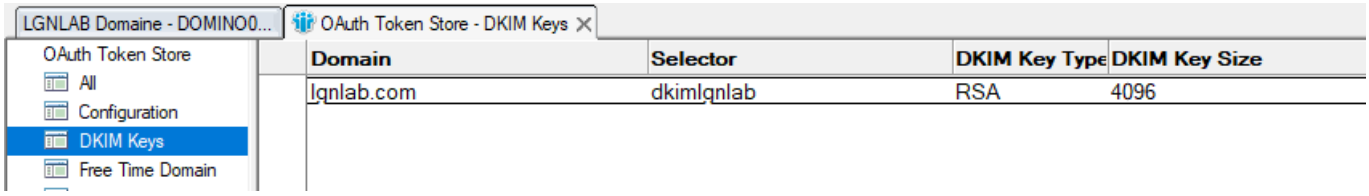
- *domain* est le nom du domaine internet
- *selector* est le nom du sélecteur que vous choisissez
- *keySize* est la taille de la clé DKIM. les tailles possibles sont 1024, 2048 et 4096

Dans notre exemple on prendre les valeurs suivantes

- *domain* : lgnlab.com
- *selector* : dkimlgnlab
- *keySize* : 4096

```
keymgmt create DKIM lgnlab.com dkimlgnlab RSA 4096
Created DKIM key dkimlgnlab._domainkey.lgnlab.com
```

La clé créé se trouve dans la base credstore.nsf dans le répertoire IBM_CredStore.



Création un enregistrement TXT DNS dans un fichier .txt

keymgmt export DKIM DNS *domain selector dkimdnsfile*

Avec

- *domain* est le nom du domaine internet
- *selector* est le nom du sélecteur que vous choisissez
- *dkimdnsfile* est le nom du fichier .txt qui contient l'enregistrement TXT DNS

Dans notre exemple on prendre les valeurs suivantes

- *domain* : lgnlab.com
- *selector* : dkimlgnlab
- *dkimdnsfile* : dkimdns.txt

```
keymgmt export DKIM DNS lgnlab.com dkimlgnlab dkimdns.txt
Parse domain lgnlab.com
Parse selector dkimlgnlab
Parse filename dkimdns.txt
Get DKIM key  d=lgnlab.com, s=dkimlgnlab, No error
Get Key as PEM No error
Get Key as DNSKey v=DKIM1; k=rsa; p=<clé publique>;
Exported DKIM key to DNS file /local/notesdata/dkimdns.txt, No error
```

Spécification de la clé à utiliser pour la signature DKIM (via notes.ini) sur le serveur.

Ajouter les informations DKIM dans la zone DNS de votre domaine.
Dans notre cas, nous allons ajouter les informations suivantes :

```
Name = dkimlgnlab._domainkey.lgnlab.com
Type = TXT
Value = "v=DKIM1; k=rsa; p=<clé publique>;"
```

Puis nous allons ajouter la ligne suivante dans le notes.ini du serveur Domino :

DKIM_KEY_<domain>=<selector>

Dans notres cas

DKIM_KEY_lgnlab.com=dkimlgnlab

Activation de la signature DKIM (via notes.ini) sur le serveur.

RouterDKIMSigning=1

Redémarrez Domino.

HCL Verse 3.0

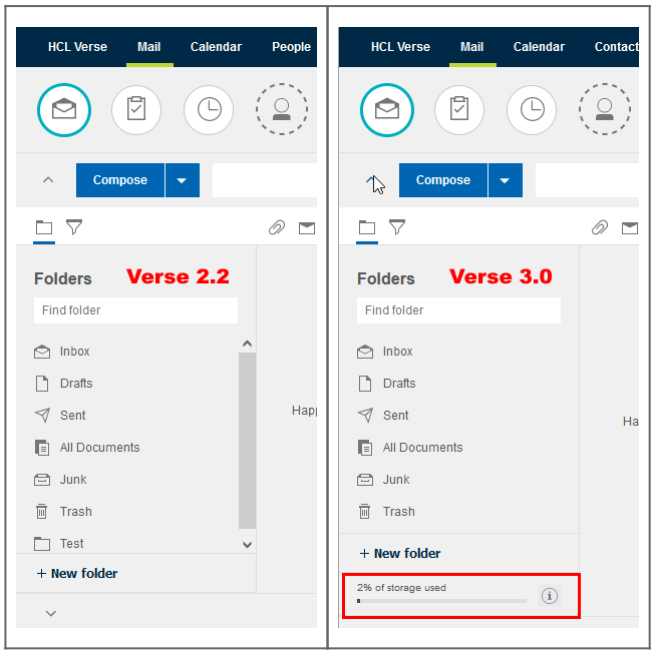
Nous allons vous présenter les principales nouveautés d'HCL Verse 3.0

1. Affichage du quota du fichier courrier
2. Création des contacts dans Verse
3. Recherche de la disponibilité lors de la planification d'une nouvelle réunion

4. Gérer les autres adresses lors de l’envoi d’e-mails
5. Définir les préférences de disponibilité
6. Utiliser l’option de discussion en mode hors ligne et du mode Ne pas déranger
7. Paramètres de courrier et d’agenda modifiés en paramètres Verse

Affichage du quota du fichier courrier :

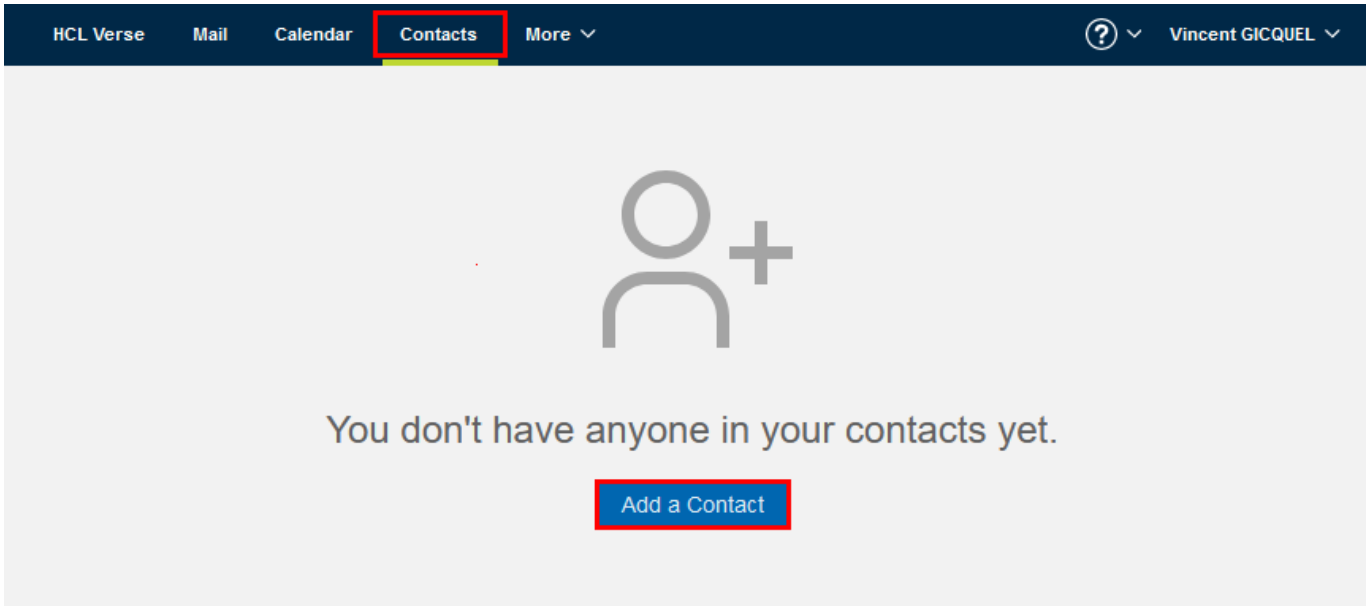
Si l’administrateur a défini un quota pour l’utilisateur, ce quota sera affiché dans Verse. Nous pouvons voir la différence sur les images ci-dessous entre la version 2.2 ou inférieure et la version 3.0.

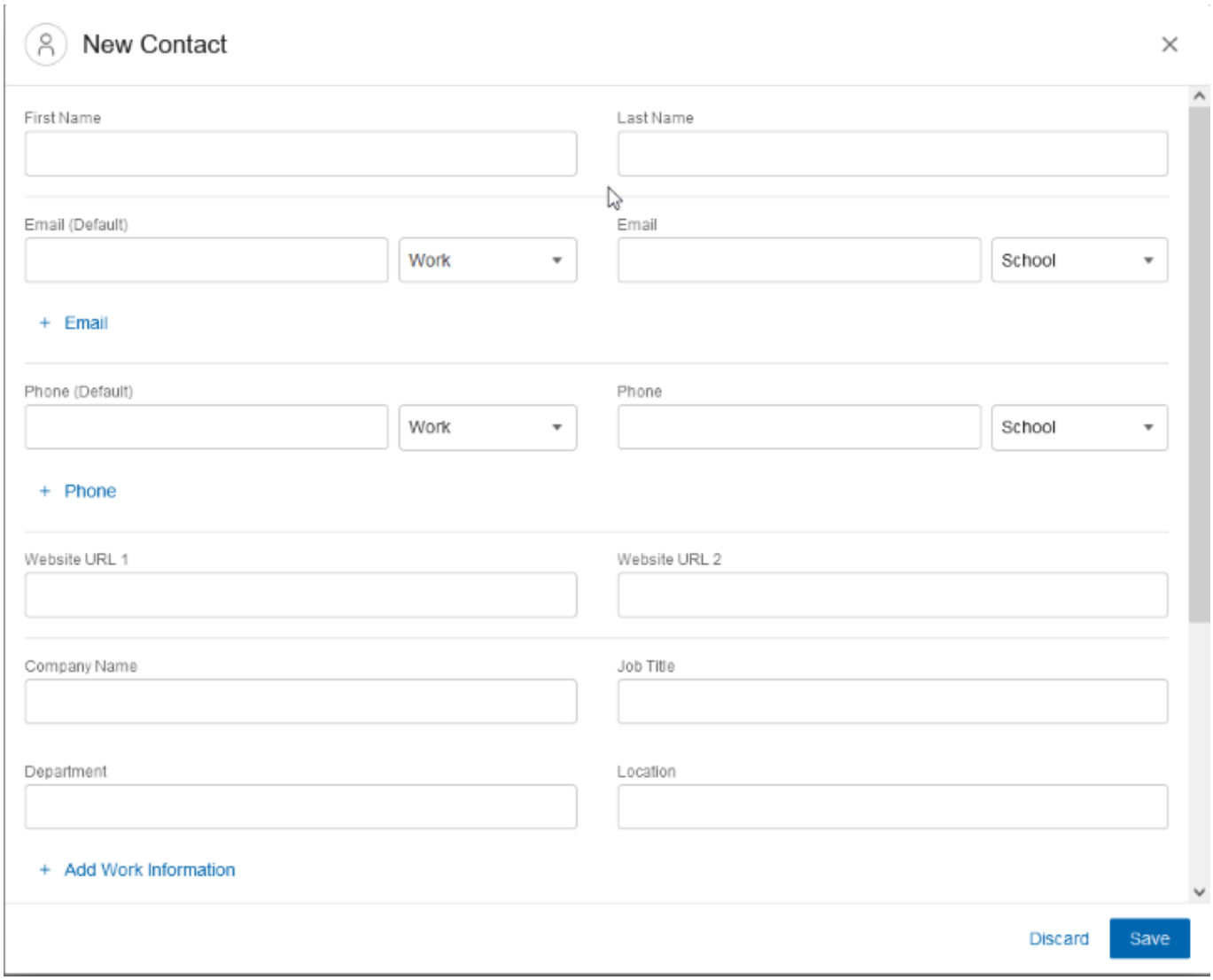


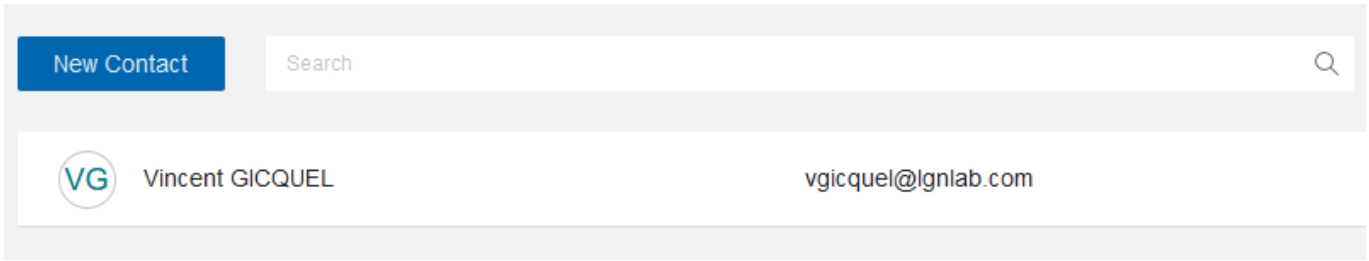
Création des contacts dans Verse :

Les utilisateurs peuvent dorénavant gérer leurs contacts à travers Verse. Il faut activer cette fonctionnalité en ajoutant le paramètre suivant dans le notes.ini du serveur Domino. Cette fonctionnalité est toujours en béta et si ce paramètre n’est pas activé, les utilisateurs peuvent toujours gérer leurs contacts via iNotes.

VOP_GK_FEATURE_201=1



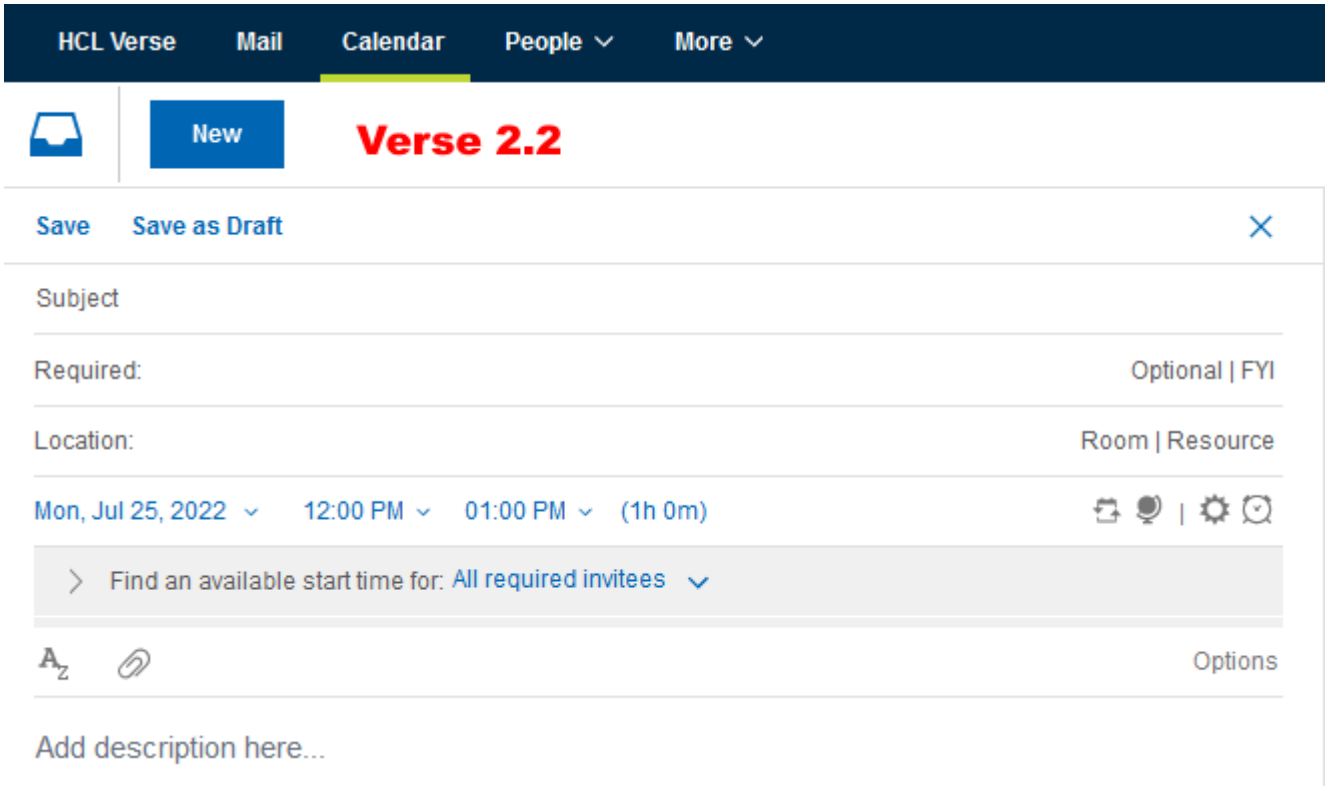


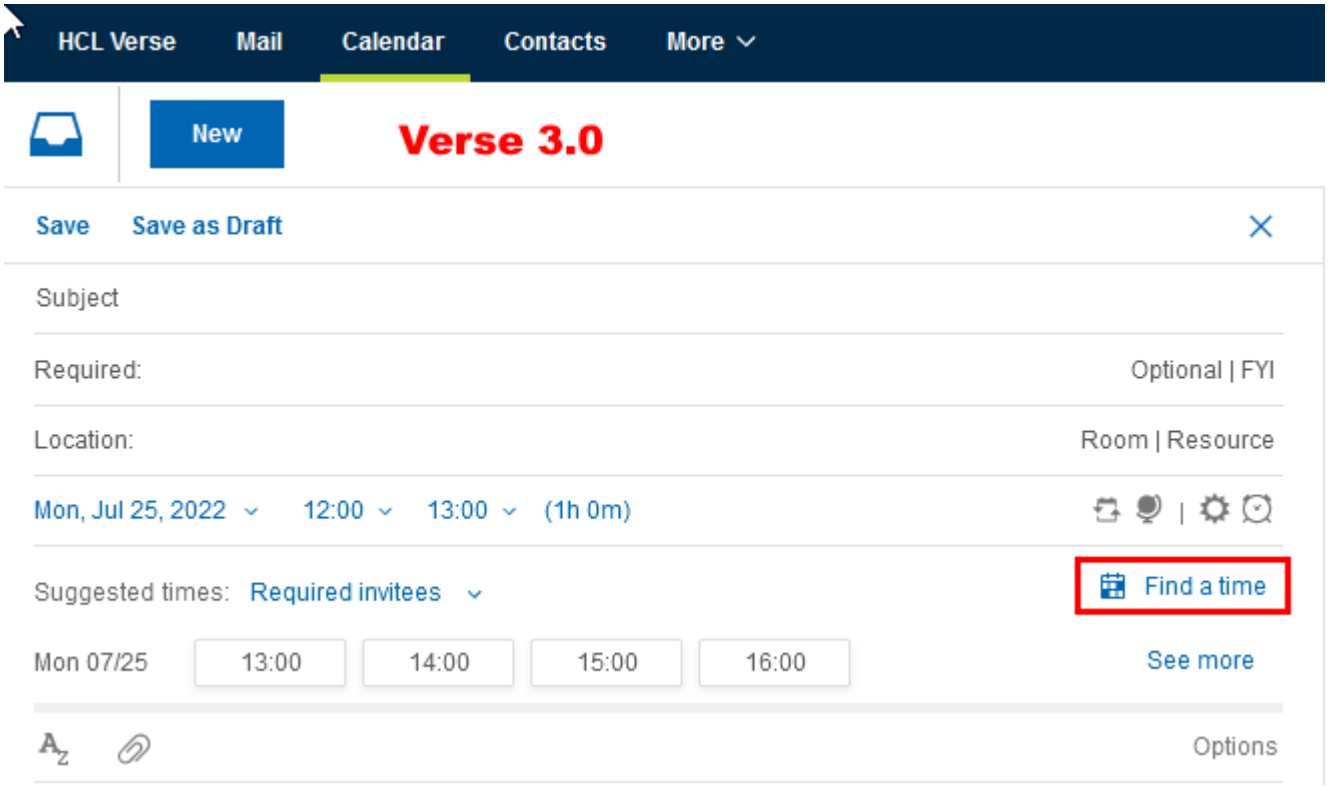


Recherche de la disponibilité lors de la planification d'une nouvelle réunion :

Les utilisateurs peuvent rechercher la disponibilité d'un invité via l'option **Find a time** ou **Rechercher une heure libre** (voir les images suivantes). Cette fonctionnalité est toujours en béta et elle n'est pas activée par défaut. Pour l'activer, il faut ajouter dans le notes.ini du serveur Domino le paramètre suivant :

VOP_GK_FEATURE_254=1



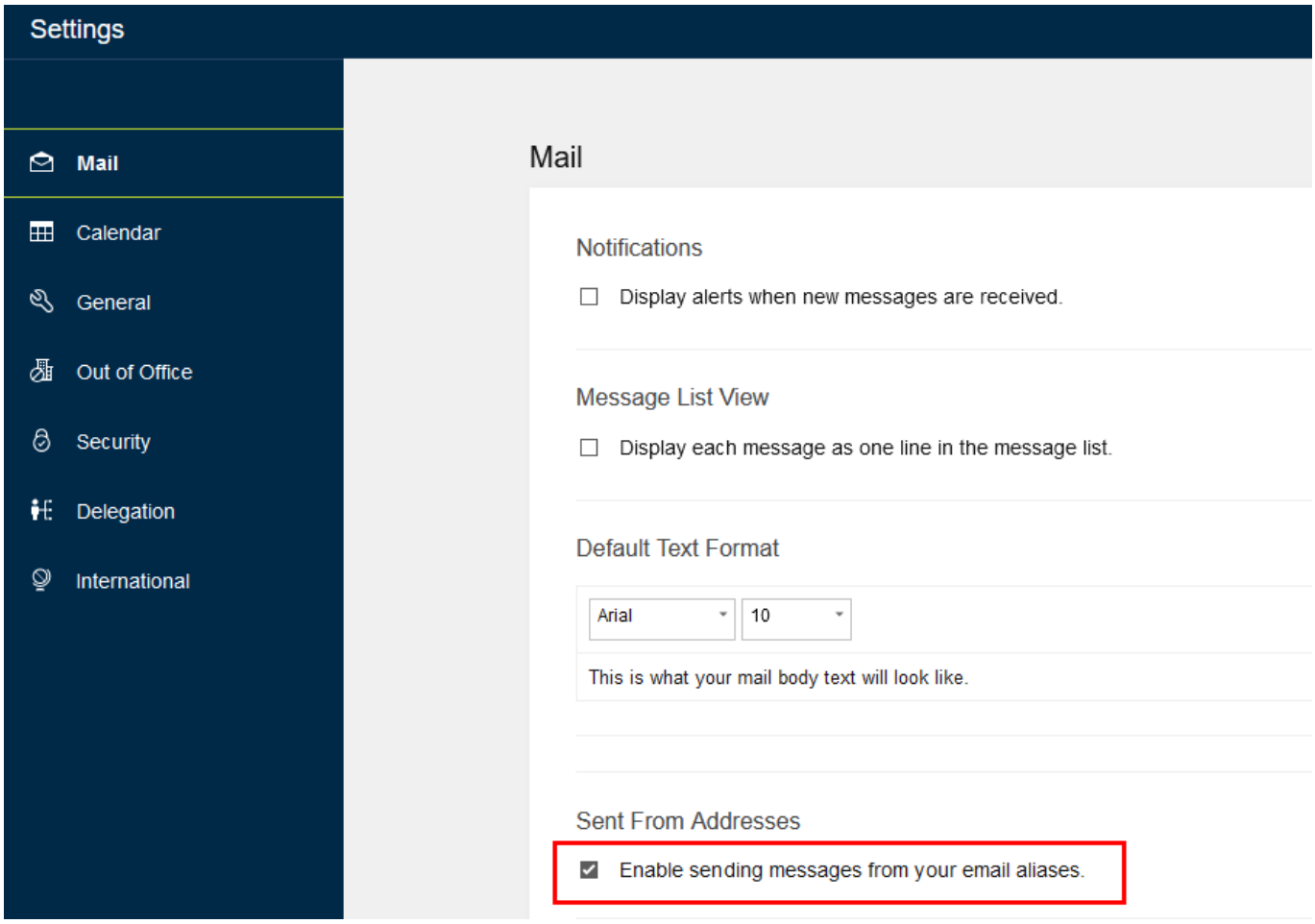


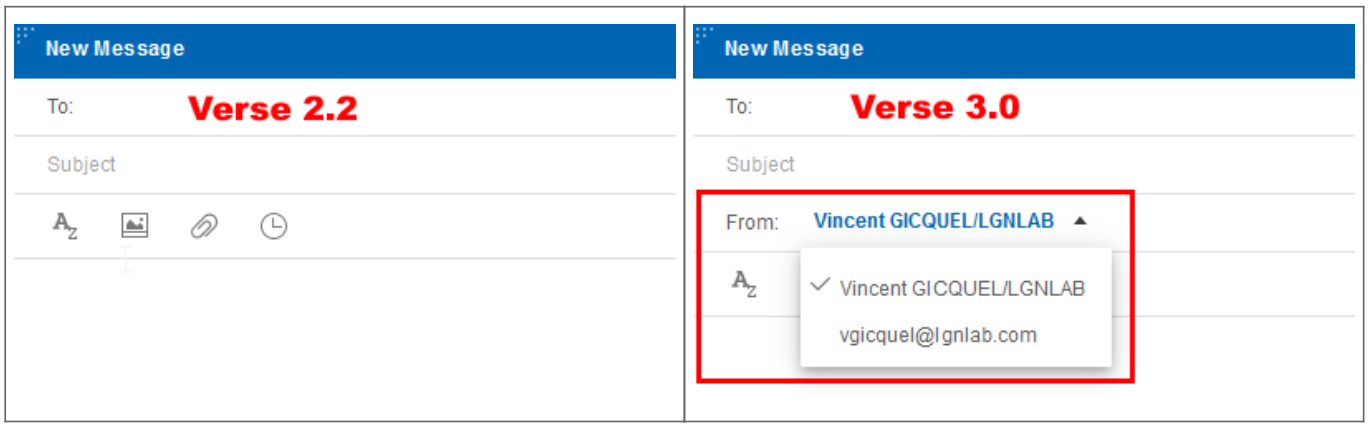
Gérer les autres adresses lors de l’envoi d’e-mails

Afin de pouvoir utiliser cette fonctionnalité, il faut que le serveur Domino soit en 12.0.1FP1 ou supérieure et que le fichier courrier soit en modèle 12. Elle permet aux utilisateurs d’utiliser une autre adresse lorsqu’ils envoient du courrier à partir de leur fichier courrier, d’un fichier courrier partagé ou d’un fichier courrier délégué.

Pour activer la fonctionnalité :

- Cliquer sur **Paramètre Verse -> Courrier (Verse settings -> Mail)**
- Dans la section **Envoyé à partir d’adresses (Sent From Addresss)**, cocher **Activer l’envoi de messages à partir de vos alias de courrier électronique (Enable sending messages from your emails aliases)**





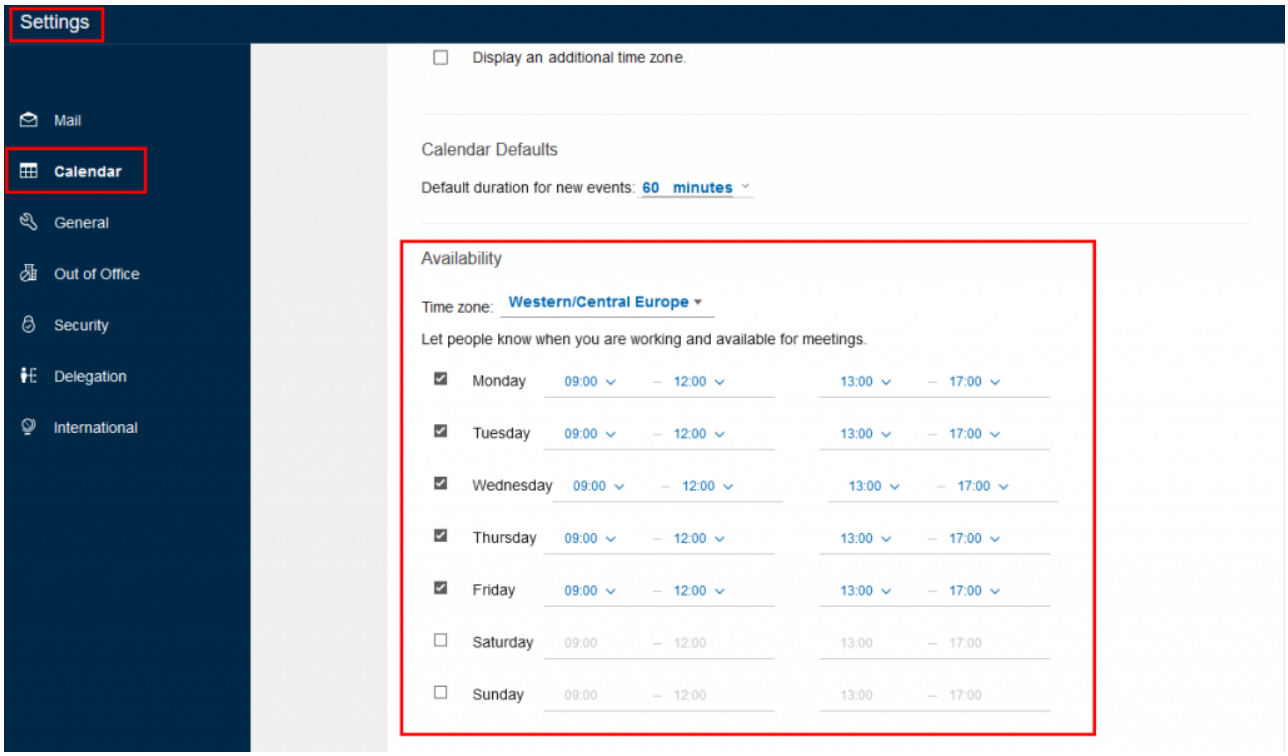
Définir les préférences de disponibilité :

Pour pouvoir utiliser cette fonctionnalité, il faut que le serveur Domino soit en 12 ou ultérieure, soit en 11.0.1FP4 ou supérieure ou 10.0.1FP8 ou supérieure. Elle permet aux utilisateurs de personnaliser leur disponibilité dans leur

fuseau horaire préféré pour informer les personnes qu'ils sont disponibles pour les réunions.

Pour activer votre disponiblité :

- Cliquer sur **Paramètre Verse -> Agenda (Verse settings -> Calendar)**
- Dans la section **Disponibilité (Availability)**, choisir son fuseau horaire et les jours de disponiblité

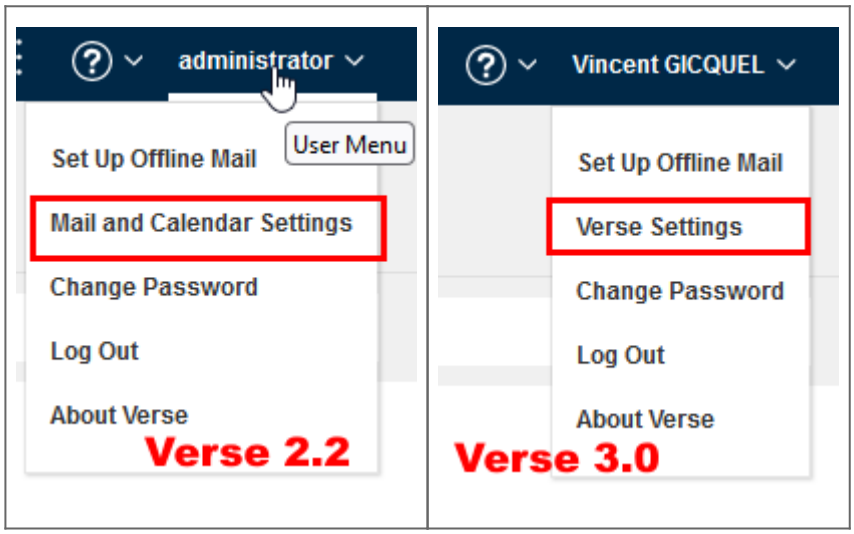


Utiliser l'option de discussion en mode hors ligne et du mode Ne pas déranger :

Pour bénéficier de cette fonctionnalité, il faut plusieurs prérequis, que le serveur Sametime soit en version 11.6.2 ou supérieure, soit en version 12 ou supérieure et que le chat persistent soit activé. Elle permet d'envoyer des messages aux utilisateurs qui sont soit hors ligne soit avec un statut Ne pas déranger.

Paramètres de courrier et d’agenda modifiés en paramètres Verse

La dernière nouveauté est le changement du titre des **Paramètres de courrier et d’agenda (Mail and Calendar Settings)** en **Paramètres Verse (Verse settings)**.



MobileIron – Ivanti – Divers

mi-access

mi-account-executive-advanced

mi-account-executive-fundamentals

mi-cloud-fundamentals

mi-core-fundamentals

mobile-threat-defense

support-specialists-fundamentals

support-specialists-intermediate

support-specialists-advanced

MobileIron – Ivanti – Cloud

01-mi-cloud

02-mi-cloud

04-mi-cloud

05-mi-cloud

06-mi-cloud

07-mi-cloud

08-mi-cloud