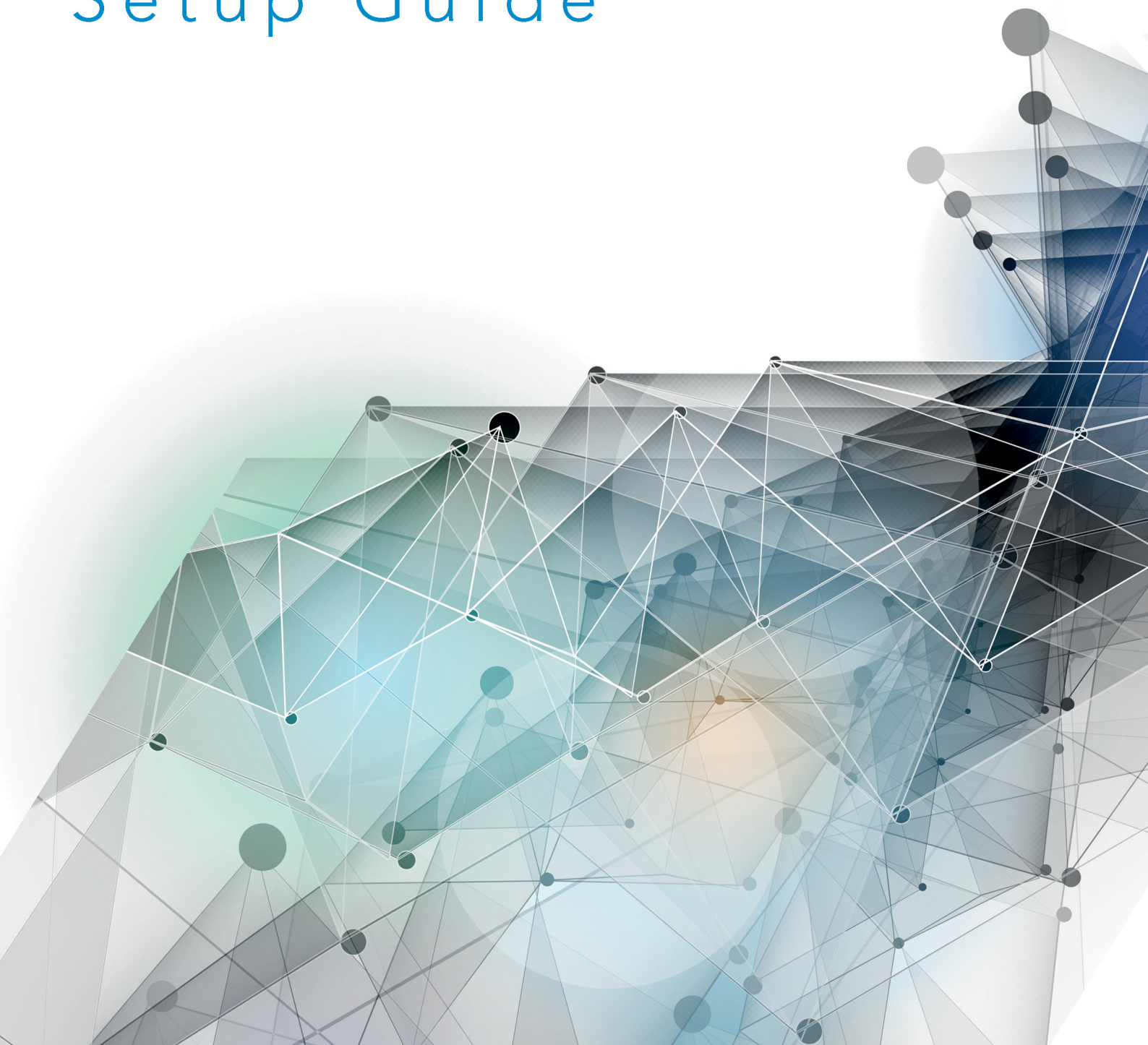
panagenda

iDNA
Applications
Setup Guide



iDNA Applications

SETUP GUIDE

Contact

panagenda Austria
(Headquarters)
panagenda GmbH
Schreyvogelgasse 3/10
AT 1010 Vienna (Austria)
Phone: +43 1 89 012 89
Fax: +43 1 89 012 89 – 15

panagenda Germany
panagenda GmbH
Lahnstrasse 17
DE 64646 Heppenheim
(Germany)
Phone: +49 6252 67939 – 00
Fax: +49 6252 67939 – 16

panagenda USA
panagenda Inc.
60 State Street
Suite 700
Boston, MA 02109 (USA)
Phone: +1 (617) 855 5961
Fax: +1 (617) 488 2292

E-Mail Sales: sales@panagenda.com
E-Mail Support: support@panagenda.com
Web: www.panagenda.com

Table of Contents

Welcome to panagenda iDNA Applications!

This guide will help you to set up panagenda iDNA Applications.

About iDNA Applications

panagenda iDNA Applications is designed specifically for managers, developers and IT administrators who are engaged in migration, optimization, modernization and transformation projects for IBM Notes and Domino applications. It uses intuitive visualizations and focused reporting to provide the information essential for ensuring projects run smoothly and achieve their goals.

In order to do so, iDNA Applications provides:

- Environment and inventory overviews
- Insights into usage from IBM Notes Rich clients and browsers
- Usage information per hierarchical department and user for analyzed databases
- Analytics on design and source code complexity
- Detailed „Design Insights" based on source code search patterns
- Design similarity and identification of „Template Candidates"
- Continuous collection of data (overview, usage and design changes)
- Platform wide code searches
- The option to **define your own custom insights, charts and dashboards**

System Requirements

Host Software

panagenda iDNA Applications comes as a virtual appliance including its own operating system based on the popular CentOS Linux distribution. No operating system needs to be prepared for the installation on the virtualization software side.

Virtual appliances are available for:

- **VMWare vSphere - ESXi** (recommended for production)

For compatibility reasons, our appliances are configured for ESXi 6.0 and Workstation 11. If you run a newer version, we recommend to upgrade the virtual machine hardware version.

- **Microsoft Hyper-V**

The underlying hardware and OS need to have VT-x support enabled (in BIOS). This is mainly relevant in scenarios where Workstation act as host software. Detailed information about operating system requirements can be found on the respective product pages: www.vmware.com/products/

Virtual Hardware

Minimum hardware requirements for production environment:

- Enterprise grade server hardware for all components
- CPU: 4 Cores
- RAM: 8 GB
- Disk: 120 GB

Adapting virtual hardware to the environment size:

Most system requirements scale with the collection period and environment size. CPU is the exception, where the four cores are adequate for most customer sizes.

Baseline Requirements:

Amount of Users	RAM	Disk Space (1 year)
Up to 5k (minimum)	8 GB	120+ GB
Up to 25k	16 GB	200+ GB
Up to 50k	32 GB	250+ GB
Up to 75k	48 GB	300+ GB
100k and above	64 GB	~5+ GB per 1k users

Disk Space per Application:

In addition to the baseline requirements, the appliance requires 75MB of disk space per database.

Partitions and disk growth:

The virtual appliance consists of several partitions for the operating system, applications, log files and the database. The database partition **/opt/panagenda/pgdata** is the only one where usage will continuously increase over time.

The application partition **/opt/panagenda/appdata** will fill quickly during the initial design collection, but usage will hardly increase after that phase.

Accordingly, disk space should be assigned as follows:

- **/opt/panagenda/appdata**: 5 MB per database
- **/opt/panagenda/pgdata**: Remainder of the disk space

See https://www.panagenda.com/kbase/x/gAK0AQ (Extending Diskspace) or instructions.

Best Practice: Leaving 10-20 GB of disk space unassigned offers a certain amount of flexibility and can help speeding up database recovery times significantly.

Deployment Example: 40k user environment with 10k database instances

- 32GB RAM
- 1 TB disk space: 250 GB (baseline) + 750 GB (10k DBs x 75 MB)
  - Leave 15 GB unassigned
  - Enlarge /opt/panagenda/appdata by 50 GB
  - Enlarge /opt/panagenda/pgdata by remaining 935 GB

Access and Permissions

IBM Domino Notes:

The following access to the Domino environment is required:

- **Single Notes ID file with access (cross certification) to all servers in scope**
  - **Reader access to at least one Domino Directory per Domain**
  - **Reader access to all servers' log.nsf databases**
  - **Reader access to all servers' catalog.nsf databases**
  - **Reader access to all servers' domlog.nsf databases where enabled**
  - **"Full Remote Console Administrator" access on all servers**
  - **Designer access to all databases where design should be analyzed**

In environments where it is not possible to grant Designer access to the uploaded Notes ID file on all focus databases, the administrator can choose to give this ID Full Administration Access per Domino server (via server document). iDNA Applications will use this access method by default if available.

Domino server requirements:

- **Statlog task scheduled on all servers**
- **Catalog task scheduled on all servers**
- **INI entry LOG_DISABLE_SESSION_INFO must <u>not</u> be set to 1**
- **"Domlog.nsf" enabled and "Access log format" set to "Extended Common"** (*names.nsf > Server Document > Internet Protocols... > HTTP*)
  MIME types "image/*", "text/css" and "text/javascript" can be excluded

Network (Firewall/Ports):

Connections to and from the appliance need to be allowed for the following services:

Outbound (originating in virtual appliance):

- Notes **RPC** to Domino servers for data collection (TCP 1352)
- **HTTP/HTTPS** to Domino servers for data collection (TCP 80/443)

Inbound (accessing virtual appliance):

- **HTTP/HTTPS** for configuration and reports (TCP 80/443)
- **SSH** for system configuration and application tuning (TCP 22)
- **VNC** for system configuration and Notes client access (TCP 5901)
- Optional: PostgreSQL for data warehouse access where enabled (TCP 5432)

It is recommended that the iDNA Applications owner has access to the console of the virtual machine (e.g. via vSphere client).
Internet access for the appliance is not mandatory, but it is recommended to grant at least proxy access to *.panagenda.com and your defined CentOS repository for security and application updates.

iDNA Applications requires the following network segments for internal communication:
- 172.17.0.1/16
- 172.18.0.1/16.
These two IP address ranges MUST NOT be routable in your production network!
Please see https://www.panagenda.com/kbase/x/mAK0AQ if they are routable.

Client System Requirements

Hardware, Operating System and Software Requirements:

The panagenda iDNA Applications web interface is based on HTML5 and therefore accessible on any **HTML5 capable device**.

- We recommend the following browsers in latest **64-bit** versions: **Chrome** and **Firefox**

Browser Security and Network Access:
No special web browser security settings are required to run the panagenda iDNA Applications web interface.
To access the web interface, you need to have access to the panagenda iDNA Applications appliance via TCP/IP, Port 80 (HTTP) and Port 443 (HTTPS).

GETTING STARTED

Setup

Please contact sales@panagenda.com to get the license and the latest versions of the following files for iDNA Applications:

- **panagenda_idna_applications_vmware_esx.ova** – image file directly deployable via the VMWare vSphere client. It holds the iDNA Applications virtual appliance in open virtualization format (OVF)
- **panagenda_idna_applications_hyperv_vhd.7z** – 7z archive which contains the iDNA Applications virtual appliance in Microsoft Hyper-V format

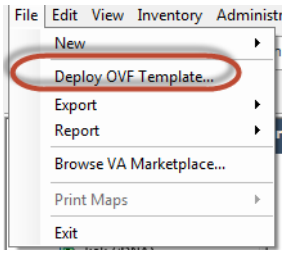
We recommend running iDNA Applications production systems in a VMWare vSphere/ESX enterprise environment. An additional option is VMWare Workstation which is mainly targeted at temporary evaluation environments and are not supported for production use.

Place the license file (*.lic) in a folder on your local hard drive. This file will be uploaded to the virtual appliance in a later step using the panagenda iDNA for application web interface.

Launching iDNA Applications using virtualization software

Recommended: VMWare vSphere/ESX via OVA

Open VMWare ESX, ESXi or vSphere and select:



The Deploy OVF Template dialog will open:

1. **Source:** Specify the location where you saved the iDNA Applications OVA file on your hard drive – for example: *C:/Temp/panagenda_idna_applications_vmware_esx.ova*

2. **OVF Template Details:** In this step you can inform yourself about the iDNA Applications version you are about to deploy. When you are done, just click on Next

3. **Name and Location:** Is the next relevant step for deploying iDNA Applications. We recommend to name this template "**panagenda iDNA Applications**"

4. **Storage:** Then you have to select a destination storage for the virtual machine files.

5. **Disk Format:** In this step, please select the storage format for the virtual disks. We recommend to choose "Thick Provision Eager Zeroed"

6. **Network Mapping:** Then select the network the deployed iDNA Applications template should use.

7. **Ready to Complete:** In the final step you are shown the options you set up. Click on Finish if you are satisfied with your setting to start the deployment task.

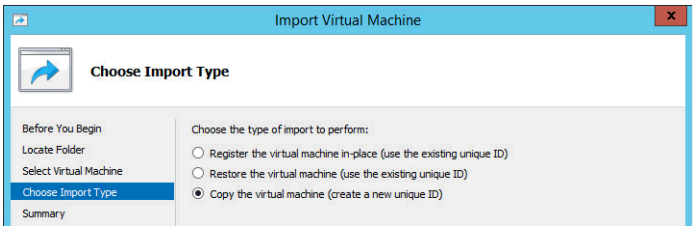
Alternative: Microsoft Hyper-V

- Extract the file **panagenda_idna_applications_hyperv_vhd.7z**

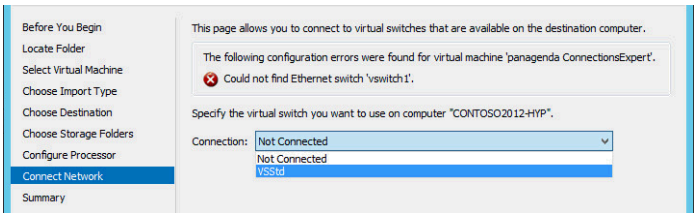
- Start Hyper-V Manager

- Right-click on your server and select "Import Virtual Machine" from the context menu

- Click **Next** on "Before you Begin" screen
- Select the folder that contains the extracted files and click **Next**
- Select the iDNA Applications image
- Select "Copy the virtual machine (create a new unique ID)"



- Click **Next** in the "Choose Destination" screen, unless you want to set the folders individually
- Select the folder where you want to store the virtual hard disk
- Click **Next** int the "Configure Processor" step – please don't change the processor settings
- Specify a network connection



Select **Finish** on the summary screen to start the copy

Alternative: VMWare Workstation/Player via VMX

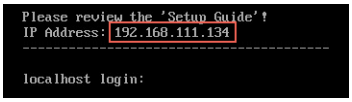
- Start VMWare Workstation
- Open Virtual Machine
- Select the file **panagenda_idna_applications_vmware_esx.ova**

Starting the Virtual Appliance

For VMWare products, we recommend raising the hardware version of the virtual machine according to your environment.
Further information: *https://kb.vmware.com/s/article/1010675*

Welcome Screen and IP Address

After starting up the appliance for the first time, you should be presented with a panagenda iDNA Applications welcome screen. If your network has a public DHCP server available, the system might already have acquired an IP address and will display the URL. **Use the shown IP address (interface URL) in your web browser to connect to the panagenda iDNA Applications web interface.** If DHCP is not available within your network or the panagenda iDNA Applications appliance did not acquire any IP address, you have to configure the panagenda iDNA Applications appliance network settings (see "Network Settings:" on page 15).



Appliance Login

iDNA Applications provides a console and a graphical user interface in order to configure operating system level settings like network, time and time zone settings.

Default login information:
user "root" with password "config"

Changing default credentials:

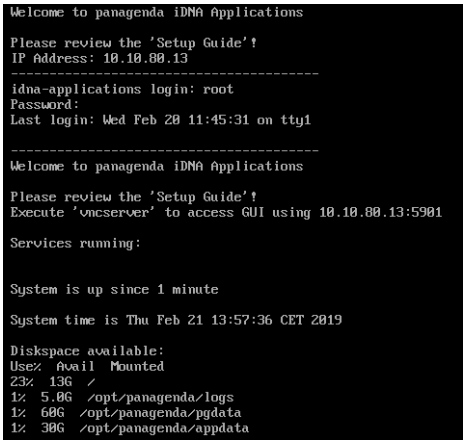
Default credentials are supplied for setup and initial configuration. It is not recommended to keep using them after the appliance has been set up.

We strongly suggest changing the default credentials for these components:

- Linux user "root" (using the "**passwd**" command)
- VNC server (https://www.panagenda.com/kbase/x/egK0AQ)
- Web user "config" (https://www.panagenda.com/kbase/x/owK0AQ)

Console

After login, basic information, such as disk space, system time and IP address, are shown:



Graphical User Interface

There are two ways to use the GUI to configure your iDNA Applications appliance:

1 **Local**

In order to start the GUI locally, enter the command "**startx**"
To start the GUI automatically when iDNA Applications is booted, please enter the following command: "**systemctl set-default graphical.target**"

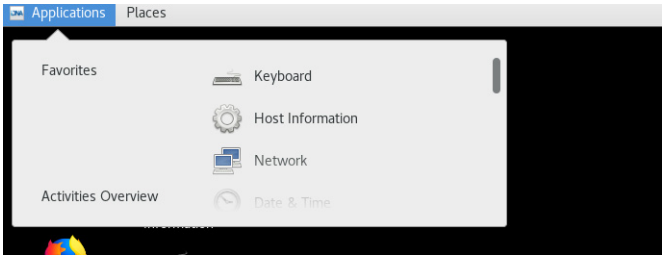
2 **Remote Access via VNC**

Please note that remote VNC access is only possible if the iDNA Applications appliance received an IP address via DHCP.

Please refer to https://www.panagenda.com/kbase/x/egK0AQ (Remote Appliance Access) for more details on VNC access.

GUI Basics

The Applications menu provides access to all required applications:



You can access all required applications by using the desktop icons, too.

To check an established internet connection, a **web browser** (Mozilla Firefox) is available on the panagenda iDNA Applications appliance.

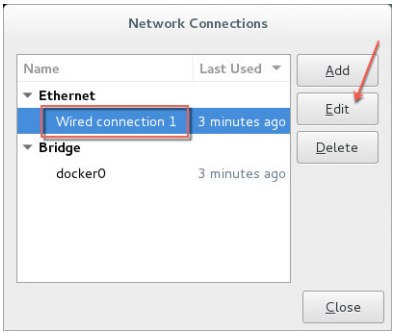
You can use the **terminal window** to check if your TCP/IP connection is established, using Linux *ping* and *ifconfig* command. For more information about *ping* and *ifconfig* commands, type *man ping* or *man ifconfig* in the terminal console window.

panagenda iDNA Applications log files can be found within the /opt/panagenda/logs directory. The main log file (idna/idna.log) holds essential information about panagenda iDNA Applications runtime behavior. Use the **Files** application to navigate to these log files.

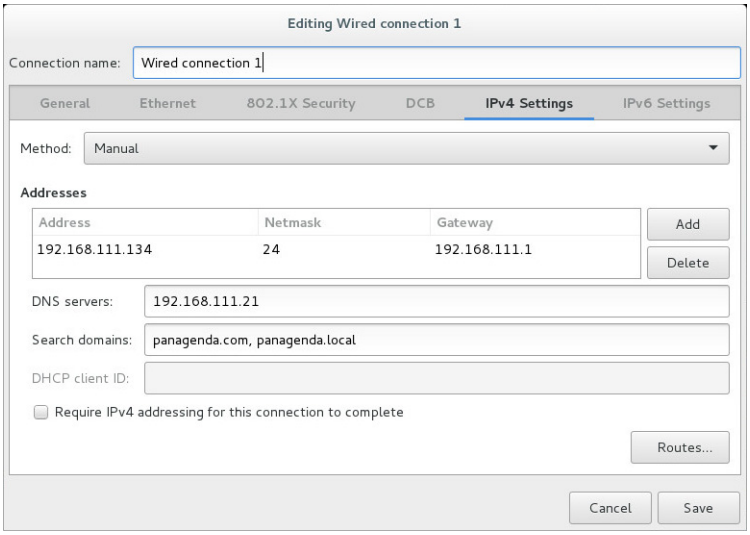
To check the panagenda iDNA Applications appliances system behavior, you can use the installed **system monitor**.

Network Settings:

To change the IP address and DNS configuration please click on the **Network** icon. Select the *Ethernet* connection and click on *Edit*:



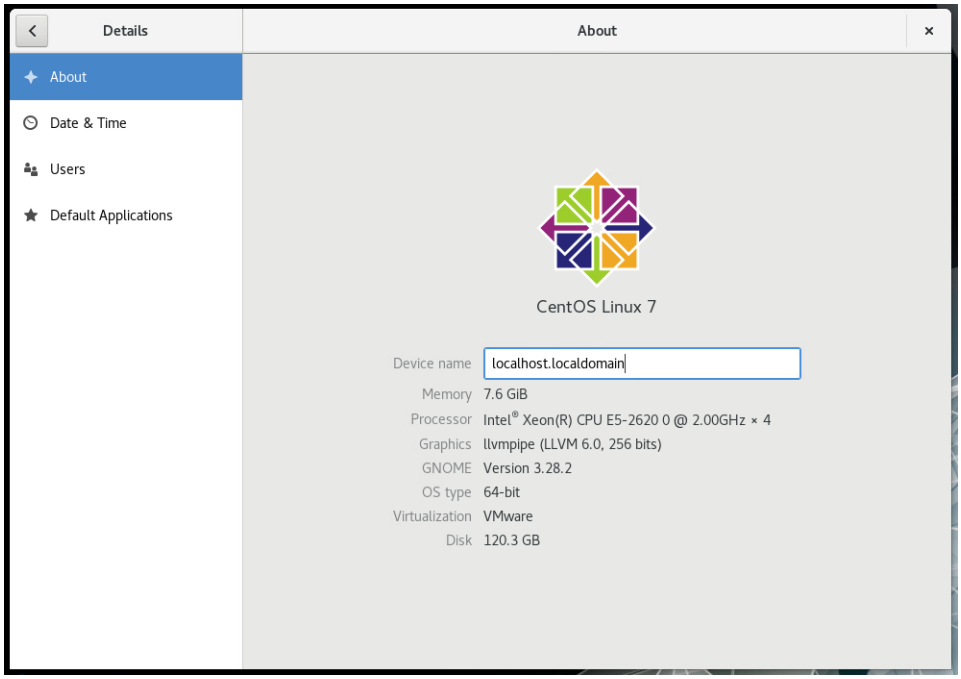
Go to the IPv4 Settings tab and select *Manual* from the *Method* drop down menu to configure the network settings as required:



TIP: If you configure "DNS Search domains", not full qualified names will also be resolved.

The virtual appliance MUST be able to resolve its own host name. Please verify that by opening a terminal window (click "Terminal" on the desktop) and using the ping command. It is recommended that both host/common name as well full qualified domain name are pingable. See "Network (Firewall/Ports):" on page 7 for incoming and outgoing network access requirements.

When changing the host name (default is "iDNA Applications") in the **Host Information** application, please make sure to adapt the host alias properties for 127.0.1.1 in /etc/hosts. This can be done using the **gedit** application. It is recommended that both host name and full qualified domain name are entered here:



Please note that the iDNA Applications notification feature uses the host name to indicate the affected appliance. For further details refer to "Setup Notifications (Mailprofile)" on page 27.

Time Zone Settings:

Please check the time zone settings of the appliance, use the **Time and Date** application to adjust.

It is very important to adjust the appliance's time zone!

Please reboot the appliance after changing the host name or date/time settings as the web server and database system require a clean start with the new configuration.

Web Interface

Please enter **https://***<FQDN or IP>* in your browser to connect to the panagenda iDNA Applications web interface. For further information about your iDNA Applications appliance's IP address, please refer to "Welcome Screen and IP Address" on page 12 and for further information about its hostname (FQDN), please refer to "Network Settings:" on page 15.

panagenda iDNA Applications uses HTTPS for secure communication between its appliance and its web interface, so you have to accept the security certificate to continue. See https://www.panagenda.com/kbase/x/fwK0AQ if you want to use your own certificate.

When you start iDNA Applications for the first time, you will see the following screen:

Please click on **Start Configuration** to open the iDNA Applications configuration portal.

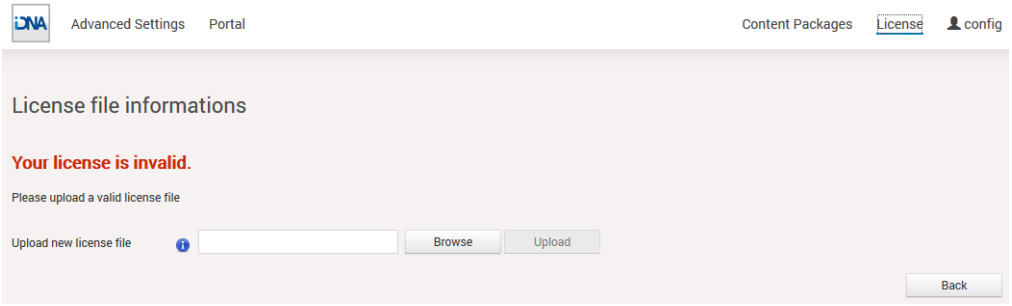
Login

By default, a user with administrative credentials is available to access the panagenda iDNA Applications web interface.

Default login information: User "config" with password "config"

License File Upload

Please go to **https://***<FQDN or IP>***/idna/cfgc#license** and upload your panagenda iDNA Applications license file when you connect to the appliance for the first time.



Note: Servers discovered, which are not covered by the license, will be shown in the list of unlicensed servers.

Content Packages – Basic Configuration

The basic configuration in this section of the iDNA Applications user interface includes:

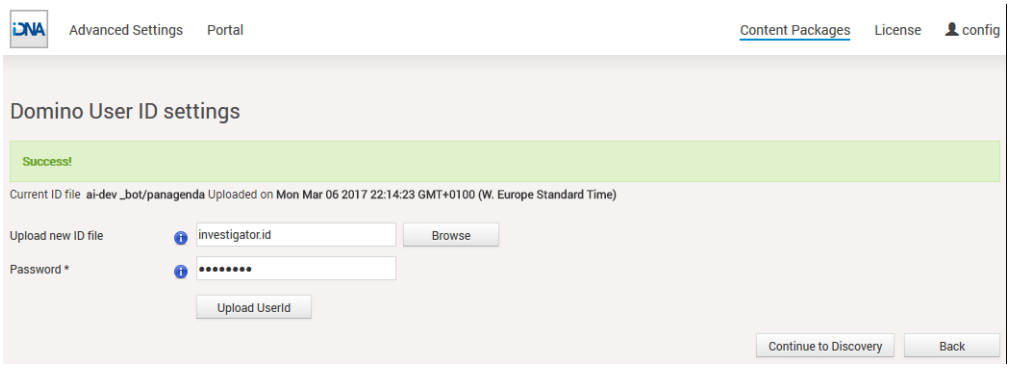
1. uploading an appropriate IBM Notes User ID
2. setting up the relevant Domino servers

1. IBM Notes User ID File Upload

In the iDNA Applications configuration portal, click on the *Setup User ID* button beside the User ID section, to open a dialog for uploading your ID file.

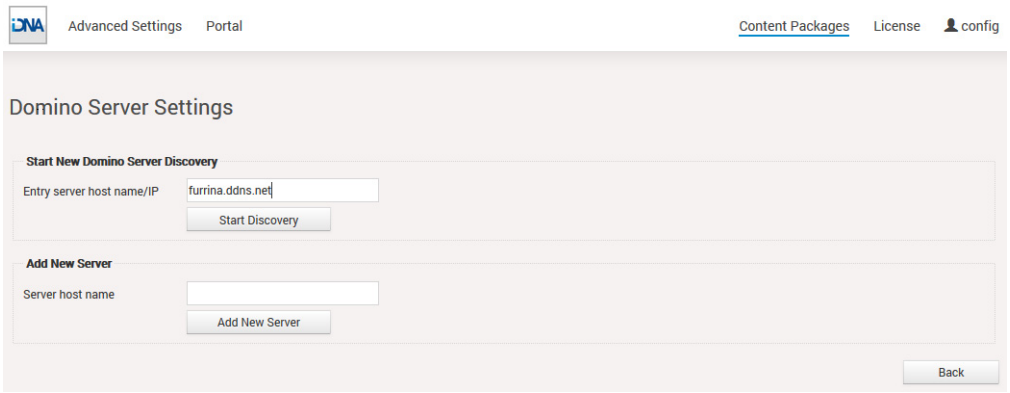
- Please ensure that the IBM Notes User ID meets the requirements (see "IBM Domino Notes:" on page 7)

To upload the new User ID file, please open the file selection dialog by clicking the *Browse* button. Select the desired IBM Notes User ID, enter the appropriate password and click on *Upload*. "Success" means that you uploaded a properly configured IBM Notes User ID:



2. Domino Server Settings

Click the *Discovery* button in the in the iDNA Applications configuration portal (https://<*FQDN or IP*>/idna/cfgc) to open the Domino Server Settings:



There are two ways to set up your Domino servers for iDNA Applications:

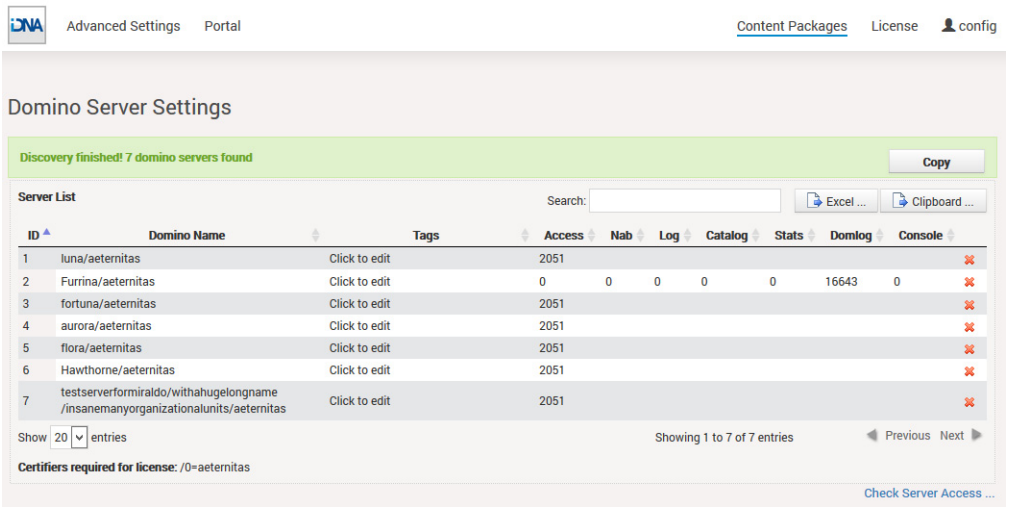
a *Start new Domino Server Discovery* – this option provides a comfortable way to add several servers to the iDNA Applications analysis

b *Add new server* – this section offers the possibility to add (further) servers manually. Just enter the FQDN of the servers iDNA Applications is supposed to analyze

Start new Domino Server Discovery

The Domino server discovery starts at the server that you enter in the *Entry server host name/ IP* field. This server's Domino Directory will be scanned for further server documents.

After entering the FQDN or IP of your desired entry server, you can start your Domino server discovery (by clicking on the *Start Discovery* button) which means that the iDNA Applications Notes client tries to access the server and reads the other server names from the server documents in its Domino directory. You will get a notification in case the iDNA Applications Notes ID doesn't have sufficient rights to access the defined entry server. Depending on your infrastructure and settings, the duration of the discovery can vary. When it is done, the results of the discovery are displayed:



In this list, all servers which have been found[1] will appear together with some information about the access status of:

- the server itself
- the log file
- the Domino Directory
- the console
- the statistics
- the domlog.nsf

If there are any access issues, they should be solved before configuring the content packages. Clicking on the red X deletes the respective server from the list. You can make use of this when you want to delete decommissioned servers that are still listed in the address book.

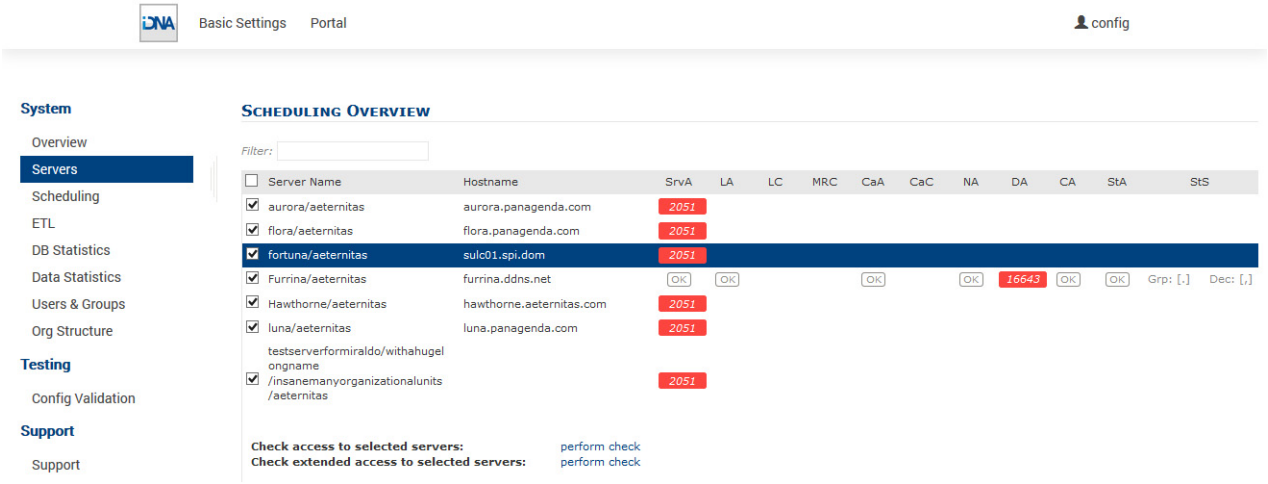
1. in the directory of the entry server of the discovery

Please note that there is a list of all certifiers displayed, which have to be included in the license file for a successful measurement.

If there are servers which could not be found in the Domino Directory of the Discovery Server you can add to them by using the ***Add new Server*** option.

Check Server Access

Clicking on the link ***Check Server Access*** on the *Domino Server Settings Result* page leads to the following screen:

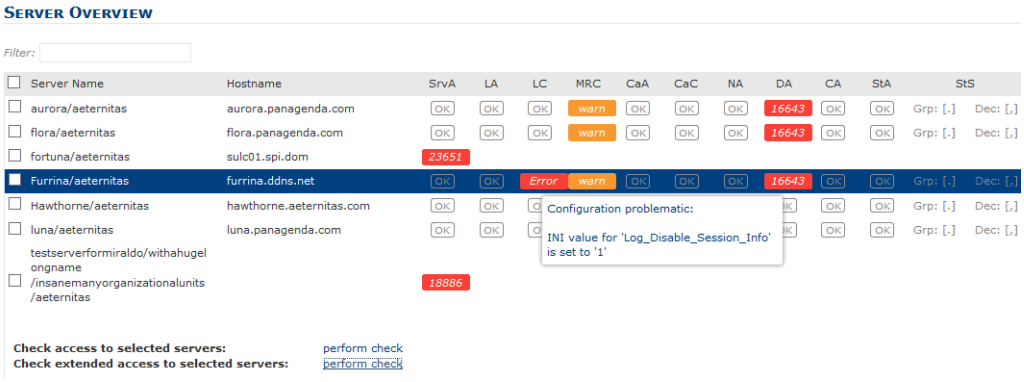


Please ensure that columns *SrV* (Server Access), *LA* (Log.nsf Access), *CaA* (Catalog.nsf Access), *NA* (Domino Directory Access), *StA* (Statlog.nsf access) and *CA* (Console Access) are showing "OK".

After fixing missing access rights for a particular server, select the server in first column and click on ***perform check*** in the line *Check access to selected servers*. This will repeat the initial access check which was done during Server Discovery (see "Start new Domino Server Discovery" on page 19).

If all access right requirements of all servers are fulfilled, please check all servers in the first column and run a ***perform check*** in the line *Check extended access to selected servers*. This

will examine several entries in the servers *notes.ini* file via console command in order to verify configuration parameters and come back with this screen:



Please ensure that all requirements for *LC* (Log configuration) and *CaC* (Catalog Configuration) are met by all servers. If there is an issue in one of those columns, hover over the entry and a pop up will display the issue found. Every time a found issue has been fixed on a server, please do a recheck **extended access** on that specific server. If the customer has scheduled Catalog and *Statlog* tasks via program document(s), it is OK for *CaC* (Catalog Config) to remain in warning state. It is always OK for *MRC* (Mail Routing Config) to remain in warning state, since mail routing information is not processed in iDNA Applications.

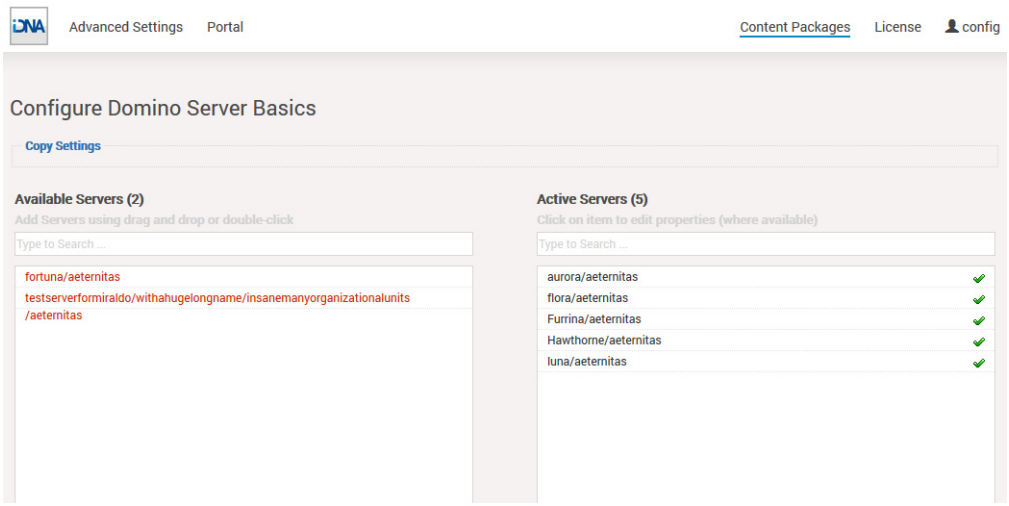
Content Packages – iDNA Applications

iDNA Applications contains the following Content Packages:

- **Domino Server Basics**
- **Database Catalog**
- **Session Activity**
- **Domino Web Log**
- **Directory/NAB Content**

With the exception of Directory/NAB and Domino Web Log content, all of them are configured as described in the following section. Directory/NAB and Domino Web Log configurations are explained in separate sections.

Configure Domino Server Basics/Database Catalog/Session Activity



To configure the Content Packages Domino Server Basics, Database Catalog, and Session Activity you only have to choose your desired servers from the list of *Available Servers*. To do so, please use drag and drop or double click on the respective servers. When you are facing a longer server list, you will also find a filter option in this configuration form as well as buttons to *Add selected* or to *Add all* servers.

From the moment you click on the *Save & Close* button, iDNA Applications will start to measure your desired servers according to the Content Package you just configured.

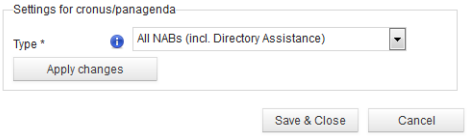
Configure Directory/NAB Content

This content package collects all Person, Group and Mail-In documents from selected Domino directories.

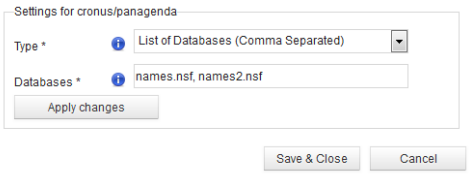
Different from most other content packages, which collect information from multiple to all servers, usually only one server per Notes Domain is selected for this content package. Typical candidates are admin servers, hubs or dedicated directory servers.

There are two options when selecting which directories are collected:

1. All address books listed in Directory Assistance (DA) of this server
   This option is the default, but may lead to undesired results if address books are part of DA which hold external persons. Only address books should be included that contain the company's own Notes users.

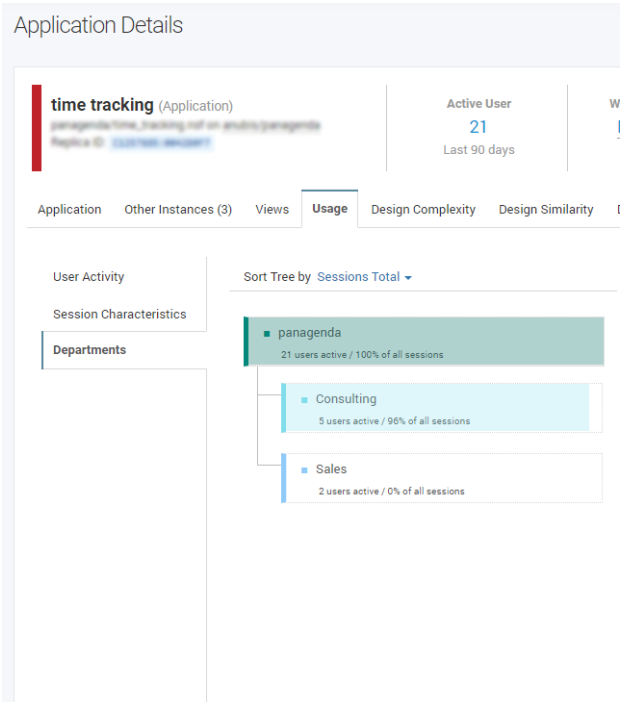


2. Comma separated list of databases
   Sometimes the better option is selecting address books manually via this option. Simply gathering "names.nsf" databases from desired Notes Domains will often provide everything that is needed.



Configuration: Usage by Organizational Units

By default, iDNA Applications automatically collects information about a user's organizational unit. This information is gathered from the Field "**Department**" in person documents in the Domino Directory. iDNA Applications aggregates this data and shows the results in the catalog:



Specify a Different Field in Person Document

If you use another person document field for organizational information, please configure iDNA Applications as follows:

- Open the file **/opt/panagenda/appdata/volumes/ai/idna/idna-config.properties** in the file system of the appliance in an editor
- Add **domino.server.nab.userdocument.import.raw=true** to enable the collection of organizational info from your organizations custom field
- Open the URL **https://***<FQDN or IP>***/idna/sys/etl**
- Click on ***Show/Hide Properties***

- **org_user_property_dep:** please enter the name of the field in the person document which holds the organizational information for that user
- **org_import_property_delimiter:** please enter the character which separates the hierarchies in the case the organization files has hierarchical content (such as the "\" in the following example "\department\team")
- **org_import_property_parsebottomup:** id info is hierarchical default order is assumed as top down if the field holds the information bottom up like (team\department\segment) please check this box

Important: After changing an entry you always have to click the corresponding update once to transfer the change into the configuration table.

Disabling the Collection of Organizational Information

If your Domino Directory's person documents do not hold valid information in the department field, and there is no other field in the person document holding that information, you can disable the collection of organizational information. If disabled, the usage by department will not be available.

Please

- Open the URL **https://***<FQDN or IP>***/idna/sys/etl**
- Click on ***Show/Hide Properties***

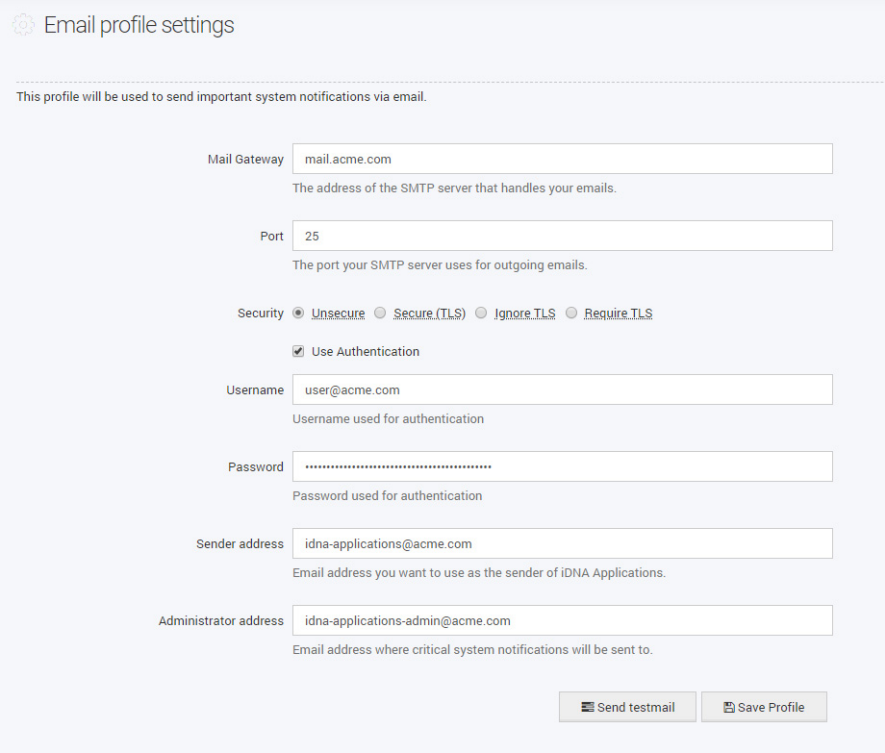
- Check **ai_department_disable_processing**
- After that you have to click the corresponding **update** link once to transfer the change into the configuration table

The changes and tweaks will be reflected in the iDNA Applications Portal after the following ETL run at 6:30 PM.

Setup Notifications (Mailprofile)

iDNA Applications requires a Mailprofile to send important system notifications, such as storage warnings, via email.

To setup a Mailprofile, click on the **Settings** icon at the right hand corner of the web interface and select **Email profile settings** from the menu:



Complete the form according to your email infrastructure. You can check your settings by clicking on the **Send testmail** button.

Click on **Save Profile** to finish the setup.

Please note that the host name of an appliance is used to identify the affected iDNA Applications installation. If the host name is configured as "iDNA Applications", which is the default value, the IP address of the appliance will be used instead. See page 16 for a description on how to adapt the host information.

Metabase

panagenda iDNA Applications includes Metabase, a fully integrated self service BI solution. It is an open source application which makes it easy to ask questions and learn from the collected data without the need of knowing SQL.

Metabase can be used right from the start without any further setup effort. More information can be found in the **panagenda iDNA Applications knowledge base**, including the default login credentials for Metabase:
https://www.panagenda.com/kbase/x/gQO0AQ

ADDITIONAL INFORMATION

Further useful information on how to get and keep panagenda iDNA Applications up and running can be found in our knowledge base:
https://www.panagenda.com/kbase/display/IA/

Especially the following topics may be relevant:

- Remote Appliance Access (VNC):
  https://www.panagenda.com/kbase/x/egK0AQ
- SSL Certificate:
  https://www.panagenda.com/kbase/x/fwK0AQ
- Extending Disk Space:
  https://www.panagenda.com/kbase/x/gAK0AQ
- Customize Docker IP Settings:
  https://www.panagenda.com/kbase/x/mAK0AQ
- Metabase Default Users:
  https://www.panagenda.com/kbase/x/gQO0AQ

DISCLAIMER

panagenda, panagenda product names and all related logos are trademarks owned by panagenda. All other names of products and enterprises in this documentation are the property of their respective owners.

panagenda reserves the right to update this documentation without being obliged to announce the changes or revisions.

Although all due care has been taken in the preparation and presentation of this documentation, the corresponding software may have changed in the meantime. panagenda therefore disclaims all warranties and liability for the accurateness, completeness, and currentness of the information published, except in the case of intention or gross negligence on the part of panagenda or where liability arises due to binding legal provisions.

Limitation of liability for external links

This documentation contains links to the websites of third parties ("external links"). As the content of these websites is not controlled by panagenda, we cannot assume any liability for such external content. In all cases, the provider of information of the linked websites is liable for the content and accuracy of the information provided. At the point in time when the links were placed, no infringements of the law were recognizable to us. As soon as an infringement of the law becomes known to us, we will immediately remove the link in question.