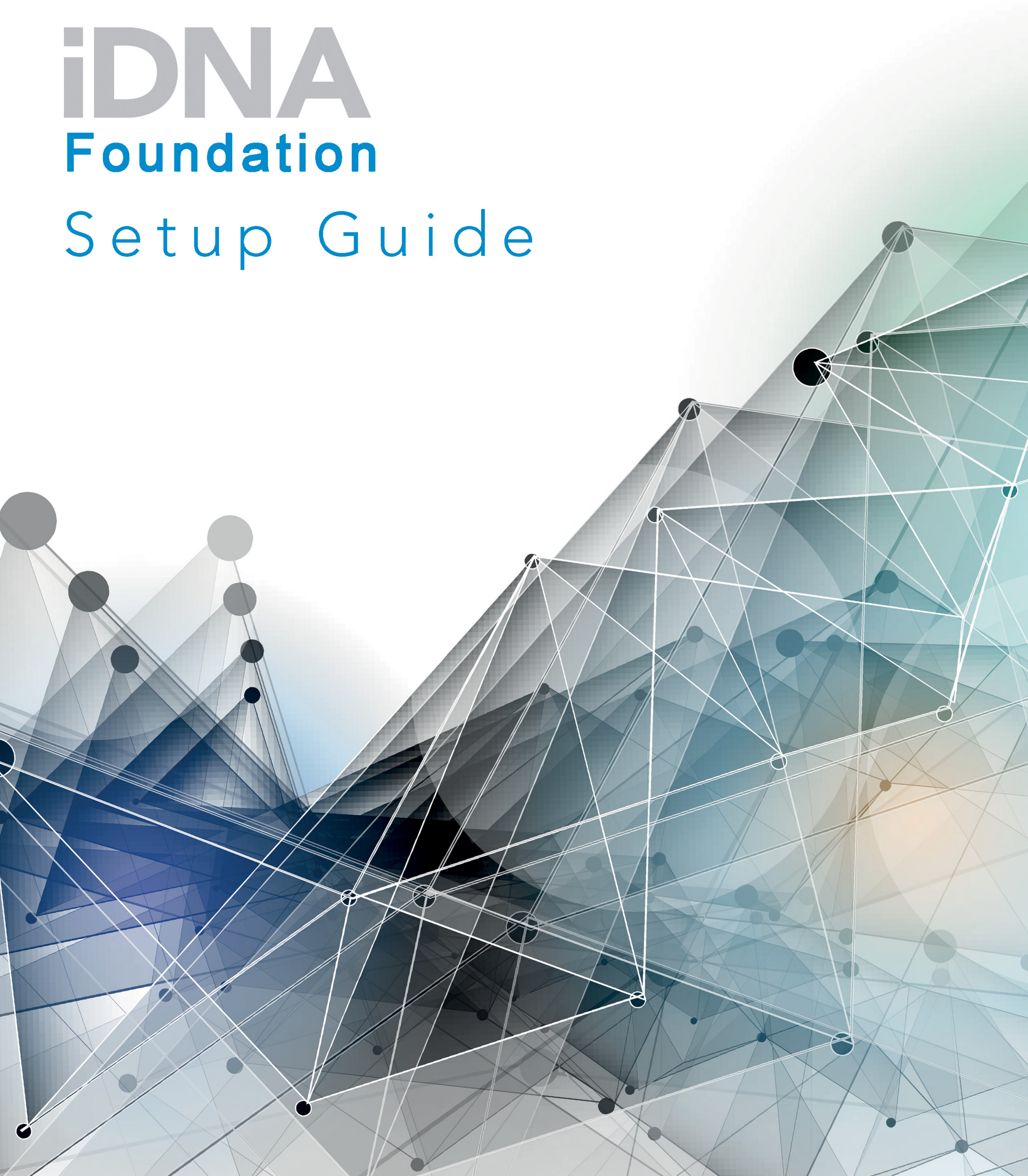
panagenda

iDNA Foundation

Setup Guide



panagenda®

iDNA

SETUP GUIDE

Table of Contents

Welcome to panagenda iDNA!

This guide will help you to set up panagenda iDNA in no time. If you have any comments or suggestions, please contact us at support@panagenda.com.

About iDNA

panagenda iDNA is a virtual appliance, which collects various infrastructure[1] information and collates it into meaningful data for use by IT departments and management. These environment reports allow you to see which applications are being actively used, which servers are barely used or not used at all, what end-user usage patterns are like, when load peaks occur, and much more.

Analysis results are possible for, but not limited to, virtually any question pertaining to IBM Notes client traffic, IBM Domino servers and application usage.

[1] Data regarding usage from log.nsf, existing data from the catalog.nsf and directories, address book information for the differentiation of mail databases and applications and for recognizing circular groups.

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
- 8 GB - 16 GB of RAM available to the virtual appliance
- 120 GB of free disk space for virtual appliance

Resource requirements vary depending on the size of the analyzed environment. panagenda and selected panagenda iDNA business partners can help you evaluate the optimum hardware specifications for your environment. As a rule of thumb a measurement's disk space requirements in megabytes can be calculated as follows: amount of servers multiplied by days of collection multiplied by ten.
For example: 40 servers * 8 days collected * 10MB = 3,200 MB

See "Extending Disk Space" on page 25 on how to extend disk space. It is not an option to add an additional disk to the system in order to provide more disk space.

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**
  - **"Full Remote Console Administrator" access on all servers**
  - **Reader access to all servers' domlog.nsf databases where enabled**

Domino server requirements:

- **Statlog task scheduled on all servers**
- **Catalog task scheduled on all servers**
- **INI entry LOG_DISABLE_SESSION_INFO must not 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 application 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 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 web interface.

To access the iDNA web interface, you need to have access to the panagenda iDNA appliance via TCP/IP, Port 80 (HTTP) and Port 443 (HTTPS).

GETTING STARTED

Setup

> ***We recommend running iDNA 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.***

Files required for initial setup:

- **panagenda_idna_vmware_esx.ova** – image file directly deployable via the VMWare vSphere client. It holds the iDNA virtual appliance in open virtualization format (OVF)
  Download URL:
  https://files.panagenda.com/iDNA/panagenda_idna_vmware_esx.ova

- **panagenda_idna_hyperv_vhd.7z** – 7z archive which contains the iDNA virtual appliance in Microsoft Hyper-V format
  Download URL:
  https://files.panagenda.com/iDNA/panagenda_idna_hyperv_vhd.7z

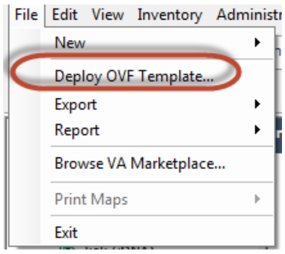
- **iDNA.lic** is your panagenda iDNA license file. Place it in a folder on your local hard drive. This file will be uploaded to the virtual appliance in a later step using the panagenda iDNA web interface

- **Notes ID** according to the requirements listed under “IBM Domino Notes:” on page 6

Launching iDNA 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 OVA file on your hard drive – for example: *C:/Temp/panagenda_idna_vmware_esx.ov*

2. **OVF Template Details:** In this step you can inform yourself about the iDNA 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. We recommend to name this template "**panagenda iDNA**"

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 template should use.

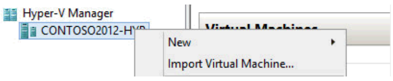
7. **Ready to Complete:** In the final step you are shown the options you set up. Click on Finish if you are satisfied with your setting to start the deployment task.

Alternative: Microsoft Hyper-V

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

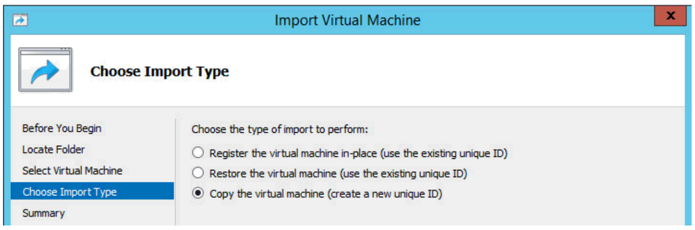
- Start Hyper-V Manager

- 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 image
- Select “Copy the virtual machine (create a new unique ID)”



Import Virtual Machine

Choose Import Type

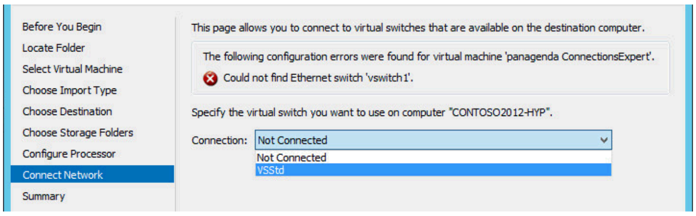
Choose the type of import to perform:

○ Register the virtual machine in-place (use the existing unique ID)

○ Restore the virtual machine (use the existing unique ID)

● 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



This page allows you to connect to virtual switches that are available on the destination computer.

The following configuration errors were found for virtual machine 'panagenda ConnectionsExpert'.

Could not find Ethernet switch 'vswitch1'.

Specify the virtual switch you want to use on computer "CONTOSO2012-HYP".

Connection: Not Connected

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_vmware_esx.ova**

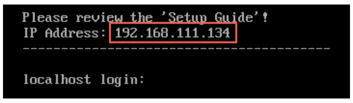
Starting the Virtual Appliance

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 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 web interface.** If DHCP is not available within your network or the panagenda iDNA appliance did not acquire any IP address, you have to configure the panagenda iDNA appliance network settings (see “Network Settings:” on page 14).



```
Please review the 'Setup Guide'!
IP Address: 192.168.111.134
----------------------------------------

localhost login:
```

Appliance Login

iDNA 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:

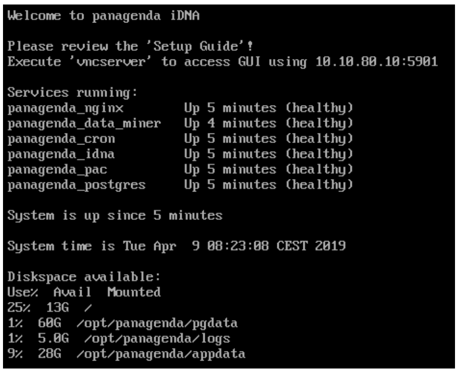
Default credentials are supplied for setup and initial configuration. It is not recommended to keep using them after the appliance has been set up.

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:



```
Welcome to panagenda iDNA

Please review the 'Setup Guide'!
Execute 'vncserver' to access GUI using 10.10.80.10:5901

Services running:
panagenda_nginx        Up 5 minutes (healthy)
panagenda_data_miner   Up 4 minutes (healthy)
panagenda_cron         Up 5 minutes (healthy)
panagenda_idna         Up 5 minutes (healthy)
panagenda_pac          Up 5 minutes (healthy)
panagenda_postgres     Up 5 minutes (healthy)

System is up since 5 minutes

System time is Tue Apr  9 08:23:08 CEST 2019

Diskspace available:
Use%  Avail  Mounted
25%  13G  /
1%  60G  /opt/panagenda/pgdata
1%  5.0G  /opt/panagenda/logs
9%  28G  /opt/panagenda/appdata
```

Graphical User Interface

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

1 **Local**

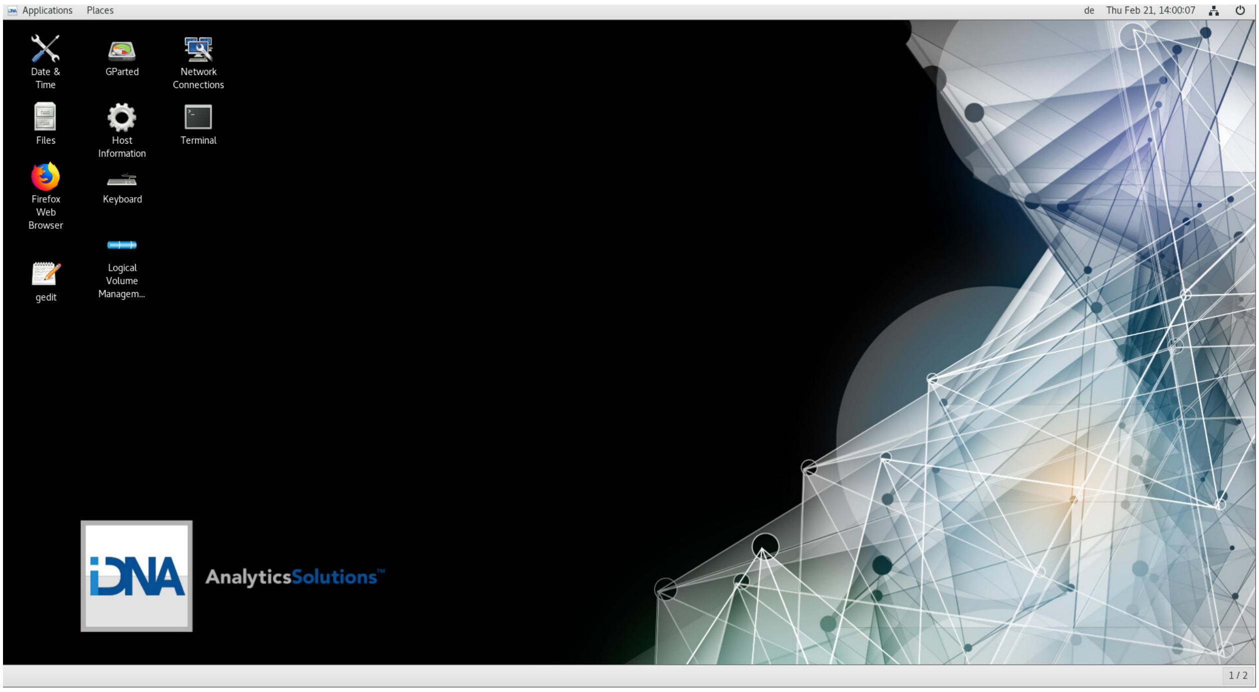
In order to start the GUI locally, enter the command "**startx**"
To start the GUI automatically when iDNA is booted, please enter the following command: "**systemctl set-default graphical.target**"

2 **Remote Access via VNC**

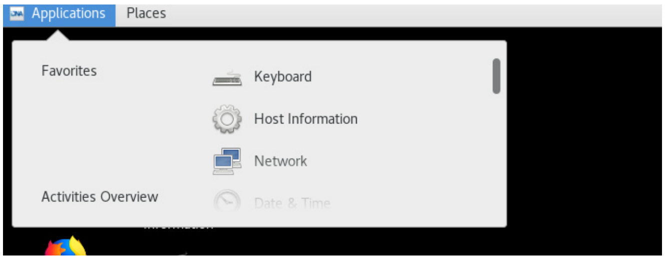
Please note that remote VNC access is only possible if the iDNA appliance received an IP address via DHCP.

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 appliance.

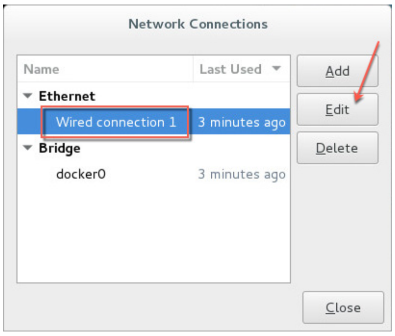
You can use the **terminal window** to check if your TCP/IP connection is established, using Linux *ping* and *ifconfig* command. For more information about *ping* and *ifconfig* commands, type *man ping* or *man ifconfig* in the terminal console window.

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

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

Network Settings:

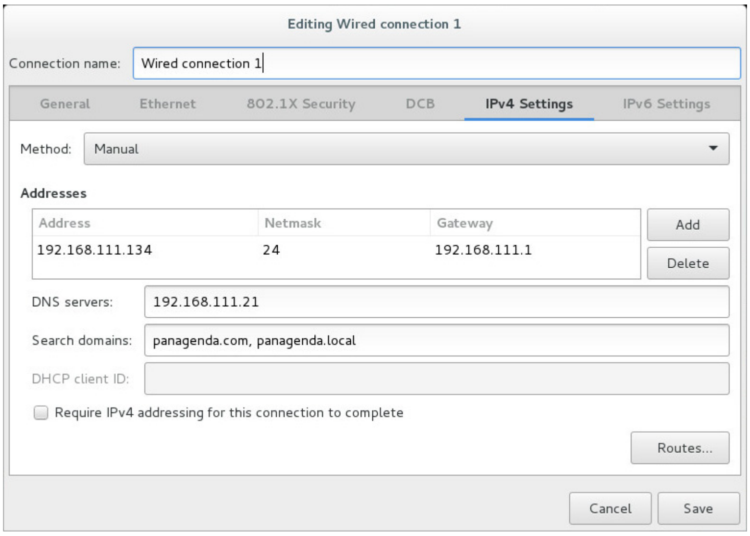
To change the IP address and DNS configuration please click on the **Network** icon. Select the *Ethernet* connection and click on *Edit*:



Network Connections

Name	Last Used
Ethernet	
Wired connection 1	3 minutes ago
Bridge	
docker0	3 minutes ago

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



Editing Wired connection 1

Connection name: Wired connection 1

Method: Manual

Addresses

Address	Netmask	Gateway
192.168.111.134	24	192.168.111.1

DNS servers: 192.168.111.21

Search domains: panagenda.com, panagenda.local

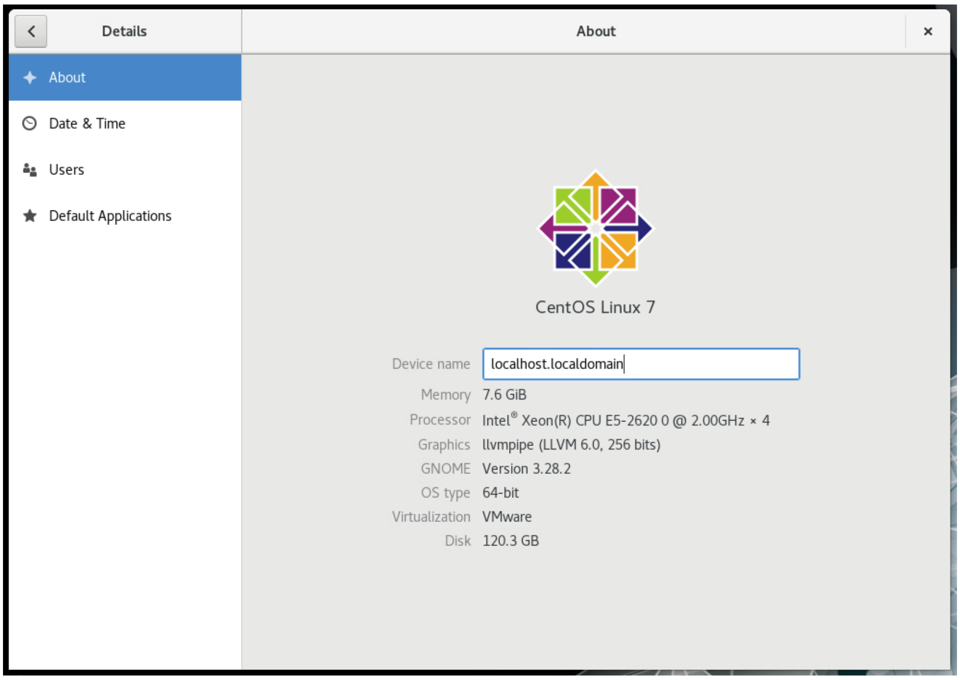
DHCP client ID:

☐ Require IPv4 addressing for this connection to complete

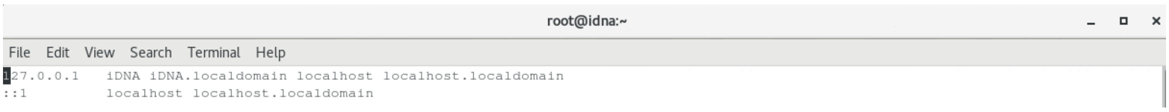
TIP: If you configure "DNS Search domains", not full qualified names will also be resolved.

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 6 for incoming and outgoing network access requirements.

When changing the host name (default is “iDNA”) 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:



Device name: localhost.localdomain
Memory: 7.6 GiB
Processor: Intel® Xeon(R) CPU E5-2620 0 @ 2.00GHz × 4
Graphics: llvmpipe (LLVM 6.0, 256 bits)
GNOME: Version 3.28.2
OS type: 64-bit
Virtualization: VMware
Disk: 120.3 GB



```
127.0.0.1   iDNA iDNA.localdomain localhost localhost.localdomain
::1         localhost localhost.localdomain
```

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 <u>host name</u> or <u>date/time</u> 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 web interface. For further information about your iDNA appliance's IP address, please refer to "Welcome Screen and IP Address" on page 11 and for further information about its hostname (FQDN), please refer to "Network Settings:" on page 14.

panagenda iDNA uses HTTPS for secure communication between its appliance and its web interface, so you have to accept the security certificate, to continue.

Login

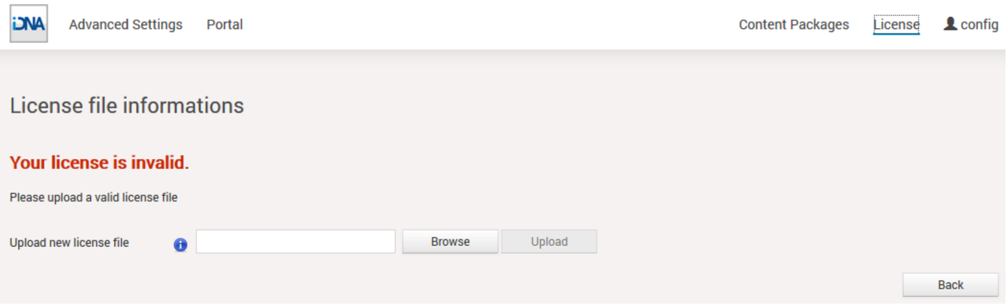
By default, a user with administrative credentials is available to access the panagenda iDNA web interface.

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 license file when you connect to your iDNA appliance for the first time.



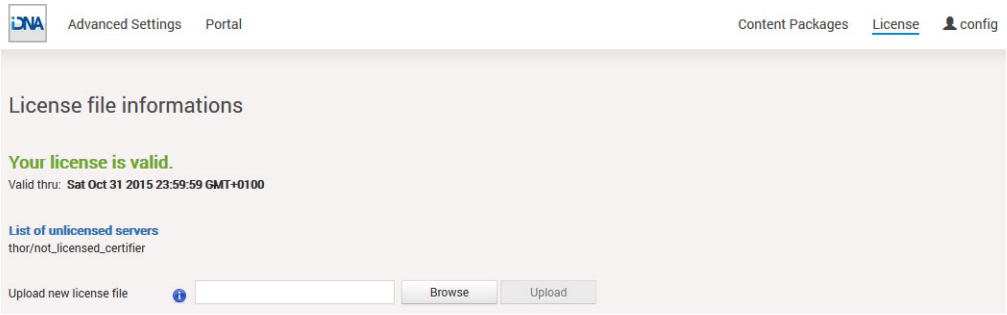
License file informations

Your license is invalid.

Please upload a valid license file

Upload new license file

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



License file informations

Your license is valid.

Valid thru: Sat Oct 31 2015 23:59:59 GMT+0100

List of unlicensed servers
thor/not_licensed_certifier

Upload new license file

Content Packages – Basic Configuration

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

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

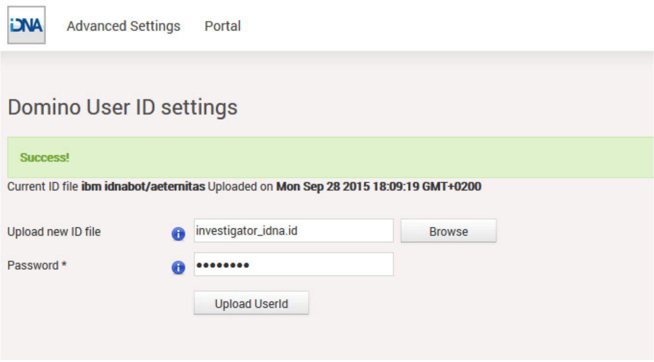
1. IBM Notes User ID File Upload

Enter **https://**<FQDN or IP>**/idna/cfgc** to get to the iDNA configuration portal. When you click on the *Setup User ID* button beside the User ID section, a dialog opens to upload your ID file.

▸ Please ensure that the IBM Notes User ID meets the following requirements:

- **access to all servers** that are relevant for the infrastructure analysis
- **read access to all log files**
- **read access to all catalog.nsf**s
- **read access to all Domino directories in scope**
- **full remote console admin rights on all servers**

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:



Domino User ID settings

Success!

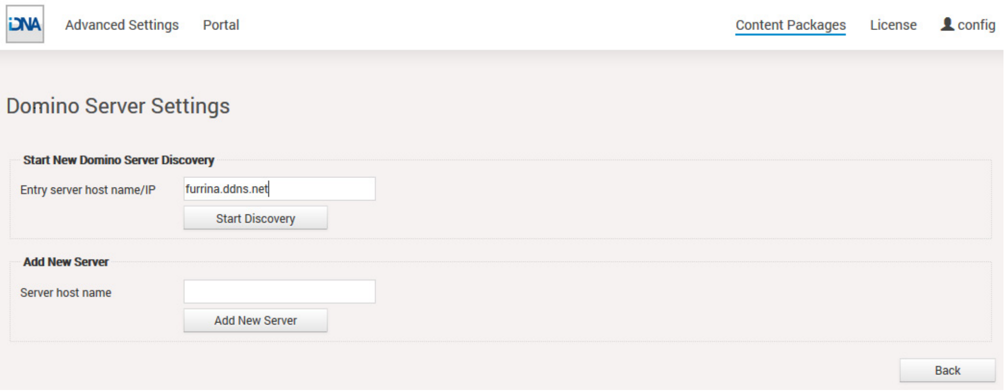
Current ID file **ibm idnabot/aeternitas** Uploaded on **Mon Sep 28 2015 18:09:19 GMT+0200**

Upload new ID file: investigator_idna.id

Password *: ••••••••

2. Domino Server Settings

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



Domino Server Settings

Start New Domino Server Discovery

Entry server host name/IP: furrina.ddns.net

Add New Server

Server host name:

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

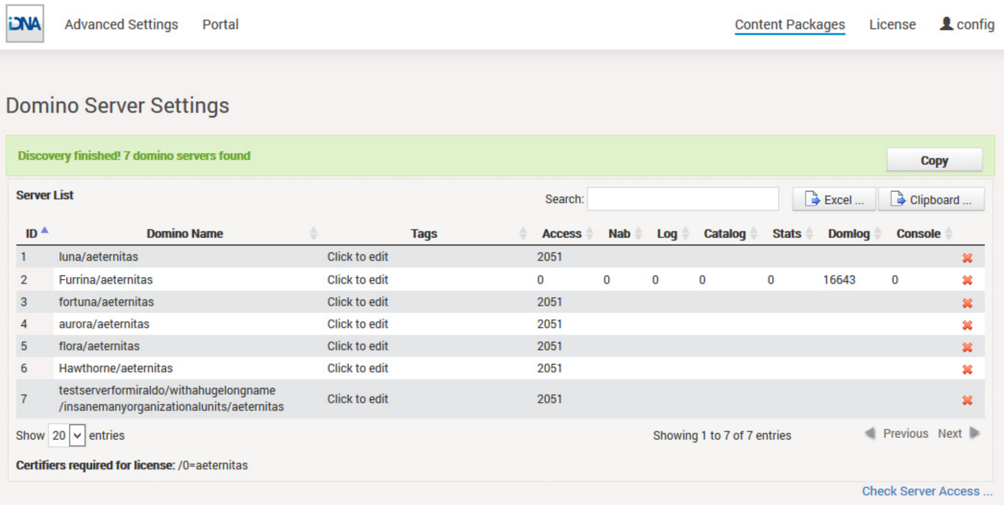
a *Start new Domino Server Discovery* – this option provides a comfortable way to add several servers to the iDNA analysis

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



Domino Server Settings

Discovery finished! 7 domino servers found

Server List

ID	Domino Name	Tags	Access	Nab	Log	Catalog	Stats	Domlog	Console	
1	luna/aeternitas	Click to edit	2051							✖
2	Furrina/aeternitas	Click to edit	0	0	0	0	0	16643	0	✖
3	fortuna/aeternitas	Click to edit	2051							✖
4	aurora/aeternitas	Click to edit	2051							✖
5	flora/aeternitas	Click to edit	2051							✖
6	Hawthorne/aeternitas	Click to edit	2051							✖
7	testserverformiraldo/withahugelongname /insanemanyorganizationalunits/aeternitas	Click to edit	2051							✖

Show 20 entries

Showing 1 to 7 of 7 entries

Certifiers required for license: /0=aeternitas

In this list, all servers which have been found[2] 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.

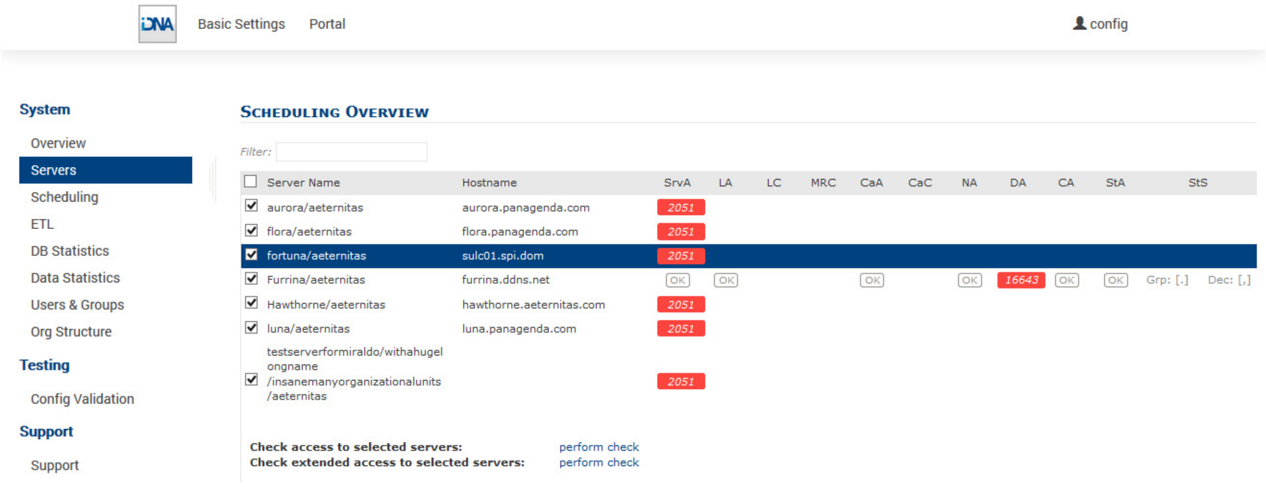
Please note that there is a list of all certifiers displayed, which have to be included in the license file for a successful measurement.

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.

[2] in the directory of the entry server of the discovery

Check Server Access

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



Scheduling Overview

Filter:

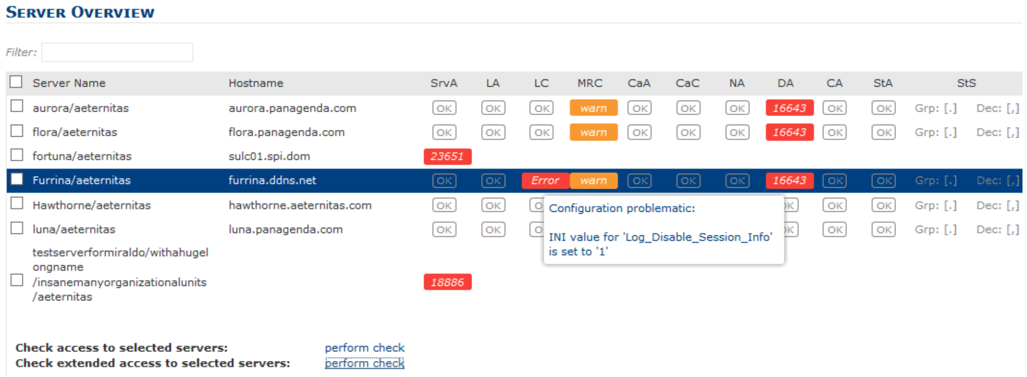
☐	Server Name	Hostname	SrvA	LA	LC	MRC	CaA	CaC	NA	DA	CA	StA	StS
☑	aurora/aeternitas	aurora.panagenda.com	2051										
☑	flora/aeternitas	flora.panagenda.com	2051										
☑	fortuna/aeternitas	sulc01.spi.dom	2051										
☑	Furrina/aeternitas	furrina.ddns.net	OK	OK			OK		OK	16643	OK	OK	Grp: [.] Dec: [,]
☑	Hawthorne/aeternitas	hawthorne.aeternitas.com	2051										
☑	luna/aeternitas	luna.panagenda.com	2051										
☑	testserverformiraldo/withahugelongname/insanemanyorganizationalunits/aeternitas		2051										

Check access to selected servers: perform check
Check extended access to selected servers: perform check

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, check mark 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 18).

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:



Server Overview

Filter:

☐	Server Name	Hostname	SrvA	LA	LC	MRC	CaA	CaC	NA	DA	CA	StA	StS
☐	aurora/aeternitas	aurora.panagenda.com	OK	OK	OK	warn	OK	OK	OK	16643	OK	OK	Grp: [.] Dec: [,]
☐	flora/aeternitas	flora.panagenda.com	OK	OK	OK	warn	OK	OK	OK	16643	OK	OK	Grp: [.] Dec: [,]
☐	fortuna/aeternitas	sulc01.spi.dom	23651										
☐	Furrina/aeternitas	furrina.ddns.net	OK	OK	Error	warn	OK	OK	OK	16643	OK	OK	Grp: [.] Dec: [,]
☐	Hawthorne/aeternitas	hawthorne.aeternitas.com	OK	OK	O					K	OK	OK	Grp: [.] Dec: [,]
☐	luna/aeternitas	luna.panagenda.com	OK	OK	O					K	OK	OK	Grp: [.] Dec: [,]
☐	testserverformiraldo/withahugelongname/insanemanyorganizationalunits/aeternitas		18886										

Configuration problematic:

INI value for 'Log_Disable_Session_Info' is set to '1'

Check access to selected servers: perform check
Check extended access to selected servers: perform check

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 IDD.

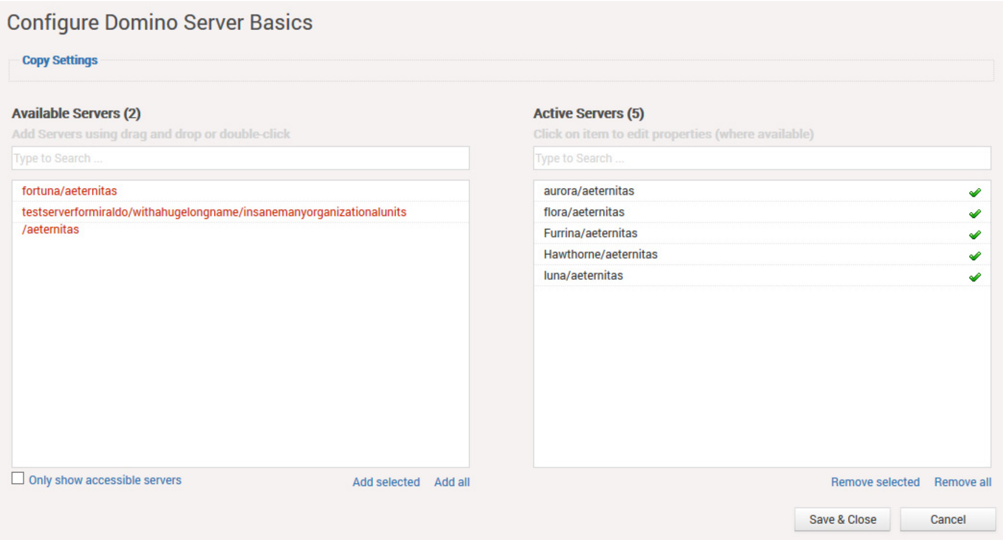
Content Packages – iDNA Foundation

iDNA Foundation 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/Domino Web Log


Configure Domino Server Basics
Copy Settings
Available Servers (2)
Add Servers using drag and drop or double-click
Type to Search ...
Only show accessible servers
Add selected
Add all
Active Servers (5)
Click on item to edit properties (where available)
Type to Search ...
Remove selected
Remove all
Save & Close
Cancel

Available Servers (2):

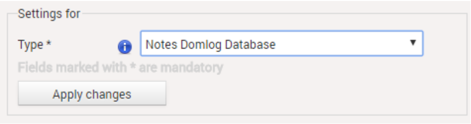
- fortuna/aeternitas
- testserverformiraldo/withahugelongname/insanemanyorganizationalunits/aeternitas

Active Servers (5):

- aurora/aeternitas ✓
- flora/aeternitas ✓
- Furrina/aeternitas ✓
- Hawthorne/aeternitas ✓
- luna/aeternitas ✓

To configure the Content Packages Domino Server Basics, Database Catalog, Session Activity and Domino Web Log, 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.

> ***Note: In the Domino Web Log configuration another section "Settings for..." will be visible. Please do not change these settings (defaults to "Notes Domlog Database").***



Settings for

Type * Notes Domlog Database

Fields marked with * are mandatory

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

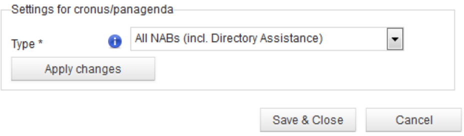
Configure Directory/NAB Content

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

It differs from other content packages, as infrastructure wide information is being gathered, which is not specific to the server from which it is collected. Therefore, only one server per Notes Domain is selected in this content package. Typical candidates are admin servers, hubs or dedicated directory servers.

There are two options when selecting which directories are collected:

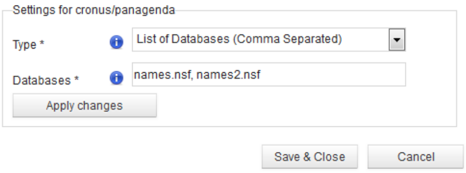
1. All address books listed in Directory Assistance (DA) of this server
   This option is the default, but may lead to undesired results if address books are part of DA which hold external persons. Only address books should be included that contain the company's own Notes users.



Settings for cronus/panagenda

Type * All NABs (incl. Directory Assistance)

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.



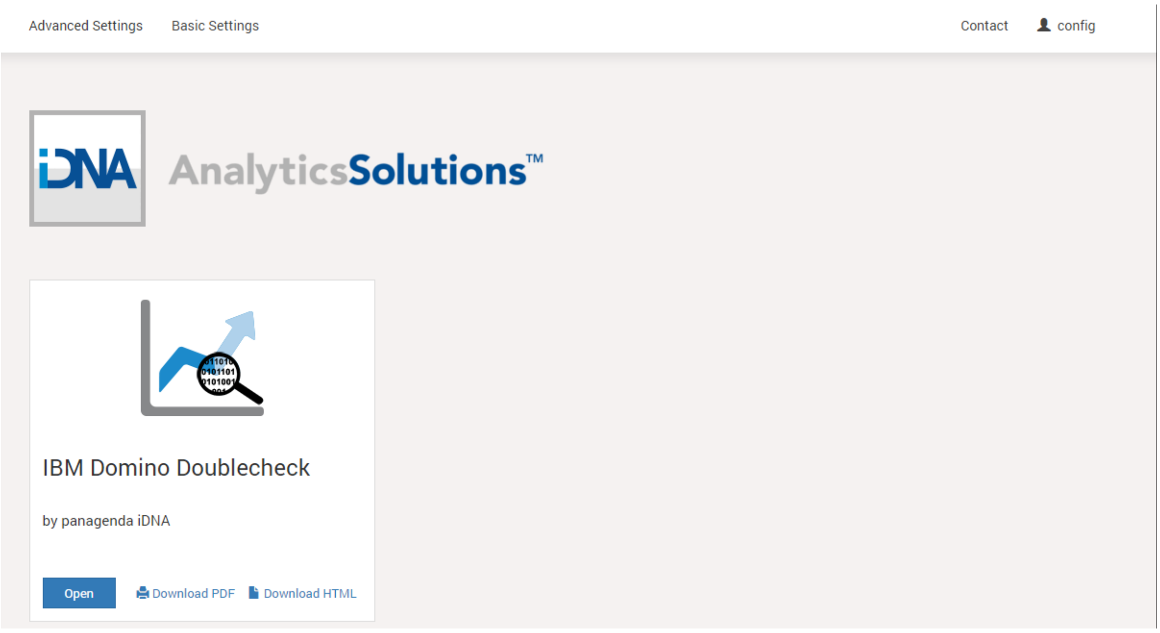
Settings for cronus/panagenda

Type * List of Databases (Comma Separated)

Databases * names.nsf, names2.nsf

Report Portal – iDNA Foundation

After the initial configuration, entering **https://**<FQDN or IP> brings you to the report portal:



Click on the Open button to open the IBM Domino Doublecheck report in a new tab/window. With Download PDF and Download HTML you can download the report in PDF or HTML format respectively.

ADDITIONAL INFORMATION

iDNA URLs

- **https://***<FQDN or IP>***/idna**
    - Home URL redirects to */idna/login*
- **https://***<FQDN or IP>***/idna/cfgc**
    - Config (Admin) Client
- **https://***<FQDN or IP>***/idna/sys**
    - System overview
    - Set of system URLs to check
- **https://***<FQDN or IP>***/idna/sys/support**
    - Download a zipped log directory to send to support!

Download Log Files

1. Log in to iDNA with your Config User and go to **https://***<FQDN or IP>***/pac/**
2. Please click the button Download next to "Download Appliance Logs"
3. Save the file to your computer

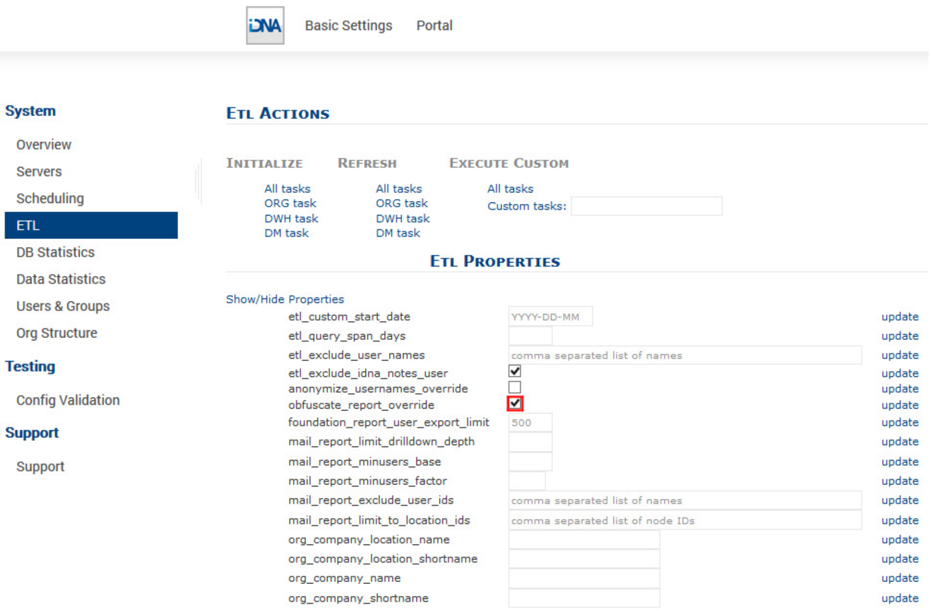
Please send this file with every support inquiry. These logs will greatly improve speed and quality of processing support tickets.

Obfuscate Report

Within iDNA, there is a way to generate an obfuscated report by configuration. This report will not contain any readable database names, database titles or user names. Therefore it can be sent out to consultants, for example, without having a data privacy issue.

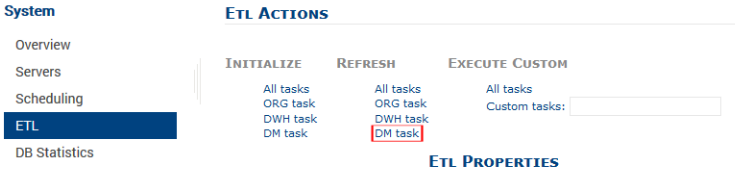
To generate an obfuscated report:

1. Go to **https://**<FQDN or IP>**/idna/**
2. Login with the known credentials
3. Goto **Advanced Settings ETL**
4. Click **Show properties**
5. Check **obfuscate_report_override** and click **update** (see screenshot on next page):



etl_custom_start_date	YYYY-DD-MM	update
etl_query_span_days		update
etl_exclude_user_names	comma separated list of names	update
etl_exclude_idna_notes_user	☑	update
anonymize_usernames_override	□	update
obfuscate_report_override	☑	update
foundation_report_user_export_limit	500	update
mail_report_limit_drilldown_depth		update
mail_report_minusers_base		update
mail_report_minusers_factor		update
mail_report_exclude_user_ids	comma separated list of names	update
mail_report_limit_to_location_ids	comma separated list of node IDs	update
org_company_location_name		update
org_company_location_shortname		update
org_company_name		update
org_company_shortname		update

6. Refresh DM by clicking **DM task** in the refresh column:



Extending Disk Space

Depending on your environment you may need to enlarge the virtual disk on which the data is stored. See the following iDNA Applications kbase entry:

https://www.panagenda.com/kbase/x/gAK0AQ

Upgrade iDNA

See the following article in the iDNA Applications kbase:

https://www.panagenda.com/kbase/x/gAK0AQ

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.