# emPass™

## v2.0

## Installation & Administrator's Guide

with

## Release Notes

DIRECTORYWIZARDS

*Published 11.28.2018*

# About this Guide

## What's in this guide?

The emPass Administrator Guide will help you:

- understand emPass and its features
- install emPass
- configure emPass
- troubleshoot issues with use of emPass

## What's not in this guide?

Not much!  This is your complete, one-stop shop for installing and using emPass.  Knowledge base articles (dirwiz.com/kb/tag/41) are published regularly when we encounter interesting client requests, though, so you may want to check them out.

## Who is this guide for?

While it is primarily intended for system/directory administrators who are already familiar with LDAP directory servers, it's also for anyone who wants to learn about and give emPass a try.  If any concept seems confusing, please contact us at support@dirwiz.com for clarification.

## How to use this guide

emPass is designed to be used with Active Directory and Office 365 currently.  More directory types available soon!  If you have a specific need, please let us know.

**IMPORTANT NOTE:** *Keep an eye out for our logo!  When you see it, we're alerting you to an important bit of information.*

## How to contact us

The best way to reach most of us all at once is by emailing support@dirwiz.com.  We can assist you via email or schedule a call or remote session if needed.

Refer to this knowledge base article (dirwiz.com/kb/418)  for information on services included with maintenance.  Visit our Support page (dirwiz.com/support) for other support options.

Have an idea for a new feature?  Is there something you wish emPass could do for you?  If you have any ideas for new features, products or even tiny utilities, let us know!  Our development team is responsive to your needs.  Contact us today at support@dirwiz.com.

# Table of Contents

# Introduction: emPass™ v2.0 release

## *Information about emPass™ v2.0 release*

emPass is a secure password synchronization tool.

This is a full release for emPass v2.0. This release supersedes all previous releases.

Please see the Deliverable Summary for information about:

- Supported Directories
- Updated Features and Functionality

## *How emPass™ works -*

emPass listens for password changes in your specified domain then replicates them to your specific target domain. Once configured for use in your environment, emPass works seamlessly to provide ongoing, secure password synchronization.

Your licensed emPass software installation will include one emPass Central Server and a minimum of one emPass Agent.

The emPass Central Server may be installed on any Windows IIS server.

Password changes are secured by HTTPS, LDAPS, and AES256 and RSA public/private keys.

Your first domain will be designated as the Source domain. Every domain controller (DC) in the source domain will host an emPass Agent to capture password changes as they occur. Your second domain requires a single DC to receives the password changes that are processed via the emPass Central Server.

Please see Appendix 1 for a diagram of a typical installation.

## *Supported Platforms and Connectivity Requirements*

- emPass for Windows will run on any Windows Server 2007 or better.
- There are several considerations for the emPass Central Server. Please see Select a Central Server in the Getting Started section for detailed information.
- The Target DC must have SSL enabled (LDAPS).
- The emPass Agent(s) must be installed on ALL domain controllers (DC) in the Source domain(s). The emPass Agent(s) must NOT be installed on the Target DC.
- Please see complete up-to-date requirements in our knowledge base (dirwiz.com/kb/3052).

## *Security*

- emPass supports LDAP directories with SSL installed and enabled.

- The SSL port number is different than a standard LDAP port number. That is, the standard LDAP port number for Active Directory (AD) and Exchange 200x (Ex200x) is 389, but the standard SSL LDAP port number is 636.
- emPass uses its own openSSL libraries (AES256 and RSA public/private keys).

Refer to Appendix B for a diagram of built-in emPass security measures.

Contact support@dirwiz.com for more information.

## *The emPass™ Maintenance Contract*

The first year of technical support and software upgrades are included upon purchase of licensing. Renew the maintenance contract yearly, and you'll continue to enjoy access to software updates as well as speedy personal email and telephone support for your question(s). Ask us anything—no request is too small—and our support specialists will get back to you with an answer.

Do you have a special request?  Is there a feature you would like to see in emPass? Just ask! Our developers are always looking for ways to make the Directify experience more personal. We'll work with you to see if enhancements are possible.

You can reach technical support Monday – Friday, 9am-5pm EST[1] via email at support@dirwiz.com or phone at 302.482.8004 (option 2 for support).

## *Licensing Requirements*

- **New User:** You will initially install emPass using a 15 day temporary key.  Following the purchase of emPass, you will receive a permanent license key.  If additional temporary keys are required for evaluation and testing, please contact us at support@dirwiz.com.  Once your purchase of emPass is complete, you will receive a permanent license key.

- **Existing emPass User:**  emPass Central Server license keys are unique to each installation, therefore, any new installation of the software, including an upgrade, requires a new license key.  You will receive a 15 day temporary key your software download, and you may request additional temporary keys while in the testing and upgrade process by contacting us at support@dirwiz.com.  Once you are satisfied with your upgrade, a new permanent key is provided upon request with a current maintenance contract.  Please send all permanent key requests to keys@dirwiz.com.

[1] excluding major US holidays and observing Daylight Savings Time (EDT)

## Licensing and Sales Inquiries

- Contact support@dirwiz.com for technical assistance.
- Contact sales@dirwiz.com for pricing and purchase inquiries.
- Contact keys@dirwiz.com for temporary and permanent keys.

# Getting Started

emPass synchronizes passwords across your enterprise quickly, easily, and securely. Planning your installation is a vital step to ensure emPass works properly right away. Please review all topics below before you begin your install.

## *Create an emPass Account for Active Directory*

Create an account that emPass will use to read and/or write to your directories. To write passwords to an AD domain, this user account must have **domain admin** privileges.

## *Select a Target Domain*

Your emPass Target Domain must have SSL enabled (LDAPS) in order to receive password changes.

## *Select a Central Server*

A few things may influence your selection of a server to use as your Central Server:

- The emPass Central Server must be installed on Windows Server 2007 or better.
- The emPass Central Server must be installed on a web server (IIS).
- The emPass Central Server must be installed on a 64-bit OS.
- The emPass Central Server must be able to connect to the emPass Target DC over the LDAPS port 636 (also known as LDAP SSL).
- The emPass Central Server does not have to be installed on a DC, but can be.
- The emPass Central Server may be installed on the emPass Target DC, but it does not have to be.
- Short downtimes are acceptable, but the emPass Central Server should be running 24/7 to capture and sync all password changes.

## *Allow for Reboot on Agent Servers*

emPass Agents are installed on each of your Source domain controllers (DC's). A **reboot is required** for each server where an Agent is installed – so please plan your installation with this required reboot in mind. emPass will not work properly without this required reboot.

# Installation and Upgrade Instructions

This release of emPass is available for download at www.dirwiz.com/download.  Upon request, you will receive an automated email which includes a link to download the software along with a 15 day temporary license key.

Depending on which type of user you are, you'll follow one of the following instructions. Click on your user type for installation instruction:

**First Time emPass-v2.0 for Windows User**

**From previous emPass versions for Windows User**

**IMPORTANT NOTE**: *If you are upgrading from any previous version of emPass, you will be performing an in-place upgrade and special attention is needed to ensure all password changes are captured and recorded on your emPass Target Domain.  Please read over all upgrade instructions thoroughly and carefully.*

**Add additional emPass Agents for Windows User**

For installation support, please contact support@dirwiz.com.

## *First Time User – Windows*

**IMPORTANT NOTE:** *emPass is installed on your Central Server first. This server **<u>must</u>** be running 24/7 to accurately sync passwords, so choose your install server wisely. Please see <u>Select a Central Server</u> for considerations in selecting an installation location.*

### Step I – Start with your Central Server installation

1. Download the latest software at <u>www.dirwiz.com/download</u>. You will want to download while on the server where you want your emPass Central Server to reside.
2. Execute the emPass install program on this Central Server. The installation wizard will guide you through installation, but there are some important points to note:

   a) You will be prompted to accept the License Agreement.

   b) The default installation directory is C:\emPass-central-server.

**NOTE:** *You may install to any directory name provided the underlying directory structure names remain as installed, but we strongly recommend keeping the default for ease of upgrades.*

   c) Two options will be checked on the next screen – *Register Eventlog Message File* and *Generate RSA Public/Private Key Pair*. Please leave these options checked and click Install.

**IMPORTANT NOTE:** *The RSA keys are literally the keys to your encrypted passwords. You are responsible for the security of these keys. You only want to generate the keys on initial installation, and **NOT again** on upgrade. If you are upgrading your emPass installation, please see* <u>Upgrade from previous emPass versions for Windows User</u>

   d) When the wizard finishes, you will see confirmation in the window that your RSA key pair was generated. Click Close.

### Step II – emPass Web Server Configuration in IIS

Once the Central Server software is installed, you need to create and configure your emPass virtual directory in Internet Information Services (IIS).

As IIS configuration is similar for all of Directory Wizards products, you'll need to download and follow instructions in the Web Server Configuration Technical White Paper, available on our website at <u>https://www.dirwiz.com/empass/doc/</u>.

**IMPORTANT NOTE:** *We strongly recommend that you use https security on your web server. Please discuss this recommendation with your local Exchange Administrator or Microsoft Technical Support with respect to your specific environment.*

## Step III – Return to Central Server for further configuration

Browse to the install directory (you selected this in Step I.2.b above)

1. Highlight and right-click the install directory to select Properties.

a) Click the Security tab.

b) Make sure the user you identified in the Web Server Configuration (Anonymous Authentication) has Full Control.

(1) If the user is not listed under Group or user names:, click Edit.

(2) Add the new user and ensure they have Full Control.

2. Open the file named key.txt and insert your emPass license key. This will be your temporary key you received upon download or from Directory Wizards Technical Support. Save and close the file.

3. Open the file named config.txt. Fill in your:

a) syslog-host IP (optional – see Syslog/Dirlog)
example: syslog-host=127.0.0.1

b) If you filled in syslog-host IP, make sure the next two parameters are also configured:

(1) syslog-port=514

(2) syslog-protocol=udp

c) activedir-url – LDAPS url of the Target DC
example: url=ldaps://hostname:636

**IMPORTANT NOTE:** *The directory name is set when the virtual directory is created in Step II. Please note the use of ldaps rather than https in the above example.*

e) activedir-id – Domain Admin account of the emPass Target DC
example: activedir-id=empassadmin@domain.com

f) activedir-pw – Domain Admin account password

g) The remaining lines should be left as their default values (leave blank where blank). These last few configuration values should **ONLY** be changed at the direction of Directory Wizards Technical Support:

(1) activedir-query=(&(objectclass=user)(samaccountname=%s))

(2) activedir-ou=

(3) activdir-srcdomain=

3. Save your config.txt changes.

Installation of the Central Server is now complete. You will need to note the hostname of the Central Server for the installation of the emPass Agents.

## Step IV – emPass Agent installation

Please ensure you have completed Steps I-III before proceeding. You will not be able to install the emPass Agents without a fully configured Central Server.

**IMPORTANT NOTE:** *The Agent must be installed on each DC on the Source in order for all password changes to be captured and updated on the Target Domain. A **reboot is required** for each server where an Agent is installed – please plan your installation with this required reboot in mind.*

1. Log into a DC where you want to install the Agent.
2. Once logged in, browse to your Central Server emPass web page.
   Example: https://hostname/emPassCS

**IMPORTANT NOTE:** *The directory name is set when the virtual directory is created in Step II. Please note the use of https rather than ldaps in the above example.*

3. Click the **emPass Active Directory Agent** link to download and install the emPass Agent on your domain controller. The installation will guide you through installation, but there are some important points to note:
   a) You will be prompted to accept the License Agreement.
   b) The default installation directory is C:\emPass-agent-ad-v# (“# ” refers to the current version number and will be followed by said version number).

**NOTE:** *You may install to any directory name provided the underlying directory structure names remain as installed.*

   c) In the Extra Options window, leave all components checked (default).
   d) Enter emPass Central Server web page (ex: https://hostname/empassCS)
   e) Click *Install*. During installation, your RSA public key will be installed automatically.
   f) You will see a pop-up window that lists the Install Serial Number of the emPass Agent. Note this Install Serial Number somewhere as you will need to manually enter it on the Central Server. Press OK.

**NOTE:** *If you neglect to note your emPass Agent Serial Number, there is a way to retrieve it via an Agent status check. Please see* this knowledge base article *(dirwiz.com/kb/3115) for more information.*

4. The installation of the emPass Agent is nearly complete. At this point, you **must** reboot the installation server before emPass will begin to work for you.

If you have additional DC's, make sure to **install the emPass Agent on ALL DC's**, following steps 1-4 above. If you fail to install an Agent on any DC or fail to reboot the server after you install an Agent, you cannot count on complete password synchronization.

## Step V – Final Central Server configuration

Finally, return to your emPass Central Server to records your emPass Agent serial numbers.

1. Open the file named agents.txt
2. List each of your Agent(s) Install Serial Numbers here, one per line.
3. Save agents.txt.

**NOTE:** *If you'd like to verify your your Central Server and Agents are communicating, see this knowledge base article (dirwiz.com/kb/3116). Change a test password on each DC that has an Agent installed and watch the changes passthrough to the Central Server, then test the new password on the Target*

That's it! emPass is completely installed and you can expect your passwords to sync to the Target Domain DC from this point forward!

## *Upgrade emPass Central Server for Windows User*

An emPass upgrade will most often consist of **ONLY** the emPass Central Server software. Agents will rarely – if ever- require an upgrade. It is common to run Agents that are an older, different version than your emPass Central Server.

### Step I – Start with your Central Server backup and software download

You must perform an in-place upgrade of the emPass Central Server with each upgrade. **DO NOT** install to a new directory! Follow the instructions below very carefully and in order.

**IMPORTANT NOTE:** *It is **VITAL** that you follow all instructions for upgrade very carefully. You **MUST** backup your current installation – please do not overlook this important step as it is the only way to step back if the upgrade is done incorrectly. If you have any questions about this requirement, please reach out to Directory Wizards Technical Support (support@dirwiz.com) prior to upgrading.*

1. Backup your current emPass installation files. See our Knowledge Base article regarding backups (dirwiz.com/kb/373) for more information on properly backing up your installation files.
2. Download the latest software at www.dirwiz.com/download. You will want to download while on the server where your emPass Central Server already resides. If you are upgrading in tandem with *moving* your emPass Central Server, please contact support@dirwiz.com before proceeding.

### Step II – Pause emPass Web Server in IIS

1. Start the IIS Manager. There are two ways to do this:
   a) From the Start page, go to Server Manager, then highlight *IIS* in the left pane. Right-click the default server shown in the *Servers* section on the right side of the window, then select *Internet Information Services (IIS) Manager*.
   b) OR from the Start Page, go to Windows Administrative Tools and double-click *Internet Information Services (IIS) Manager*.
2. In the IIS Manager window, expand the default server.
3. Now expand *Sites*.
4. Highlight the *Default Web Site*. You can pause the web server in one of two ways:
   a) With the *Default Web Site* highlighted, you'll see a left Actions pane. Under Manage Website, click Stop.

   OR

b) Right-click the *Default Web Site*, selected Manage Website, then Stop.

## Step III – Return to Central Server for installation

1. Execute the emPass install program on your Central Server. The installation wizard will guide you through installation, but there are some important points to note:

    a) You will be prompted to accept the License Agreement.

    b) The default installation directory is C:\emPass-central-server. If this is NOT the name of your existing directory, make changes here to install to the existing directory name, to overwrite your current installation.

**IMPORTANT NOTE:** *You* ***MUST*** *install to the existing directory name. Any other type of installation will require technical assistance to ensure password changes are not lost during the upgrade process. If you have any questions about this requirement, please reach out to Directory Wizards Technical Support (support@dirwiz.com) prior to upgrading.*

    c) On the next screen, you will see *Register Evenlog Message File* checked, and *Generate RSA Public/Private Key Pair* unchecked. **Leave these default selections** and click *Install.*

2. Browse to the install directory.
3. Open the file named key.txt and insert your emPass license key. This will be your temporary key you received upon download or from Directory Wizards Technical Support. Save and close the file.

## Step IV – Restart emPass Web Server in IIS

1. Return to the IIS Manager.
2. In the IIS Manager window, expand the default server.
3. Now expand *Sites.*
4. Highlight the *Default Web Site.* You can restart the web server in one of two ways:

    a) With the *Default Web Site* highlighted, you'll see a left Actions pane. Under Manage Website, click Start.

    OR

    b) Right-click the *Default Web Site*, selected Manage Website, then Start.

Upgrade of the Central Server is now complete. Password changes should now be handled by the upgraded emPass Central Server.

## *Add additional emPass Agents for Windows User*

This section pertains to adding additional emPass Agents after you've already been running emPass successfully. This may be needed if a new DC is added in your Source domain, as an Agent must be installed on each DC on the Source in order for all password changes to be captured and updated on the Target Domain.

If you have not yet followed instructions to install and configure your emPass Central Server, refer to the steps required for initial instructions for a First Time User. You cannot install Agents unless your Central Server is already installed and configured.

**IMPORTANT NOTE:** *A **reboot is required** for each server when an Agent is installed – please plan your installation with this required reboot in mind.*

### Step I – Install the Agent

1. Log into the DC where you want to install the Agent.
2. Once logged in, browse to your Central Server emPass web page.
   Example: https://hostname/emPassCS

**IMPORTANT NOTE:** *The directory name is set when the virtual directory was created during your initial emPass Central Server installation. Please note the use of https rather than ldaps in the above example.*

3. Click the *emPass Active Directory Agent* link to download and install the emPass Agent on your domain controller. The installation will guide you through installation, but there are some important points to note:

   a) You will be prompted to accept the License Agreement.

   b) The default installation directory is C:\emPass-agent-ad-v#. "# " refers to the current version number and will be followed by said version number.

**NOTE:** *You may install to any directory name provided the underlying directory structure names remain as installed.*

   c) In the Extra Options window, leave all components checked (default).

   d) Enter emPass Central Server web page (ex: https://hostname/empassCS)

   e) During installation, your RSA public key will be installed automatically.

   f) You will see a pop-up window that lists the Install Serial Number of the emPass Agent. Note this Install Serial Number somewhere as you will need to manually enter it on the Central Server. Press OK.

**NOTE:** *If you neglect to note your emPass Agent Serial Number, there is a way to retrieve it via an Agent status check. Please see* this knowledge base article *(dirwiz.com/kb/3115) for more information.*

4. The installation of the emPass Agent is nearly complete. At this point, you **must** reboot the installation server before emPass will begin to work for you.

If you have additional DC's, make sure to **install the emPass Agent on ALL DC's**, following steps 1-4 above. If you fail to install an Agent on any DC or fail to reboot the server after you install an Agent, you cannot count on complete password synchronization.

## Step II – Record the new Agent in the Central Server

Open your emPass Central Server to record your emPass Agent serial numbers.

1. Open the file named agents.txt
2. List the new Agent(s) Install Serial Numbers here, one per line.
3. Save agents.txt.

**NOTE:** *If you'd like to verify your your Central Server and Agents are communicating, see this knowledge base article (dirwiz.com/kb/3116). Change a test password on each DC that has an Agent installed and watch the changes passthrough to the Central Server, then test the new password on the Target*

## Syslog/Dirlog

emPass includes a basic syslog program called dirlog.exe, which installs automatically with both server and Agent.  EmPass automatically sends syslog events via UDP port 514 and dirlog.exe sends to localhost.

You can alter the configuration to send to a different host, utilize an alternate port, or send via TCP if you'd like.  In the emPass Central Server config file, you'll find the following lines:

```
syslog-host=127.0.0.1
syslog-port=514
syslog-protocol=udp
```

Simply make the changes you desire here and save your new config.txt.

Check your syslog messages from the command line by typing:

```
run dirlog
```

Leave the window up and as emPass is used, you'll see messages here.  If you'd like to verify your your Central Server and Agents are communicating, see this knowledge base article (dirwiz.com/kb/3116).

# Deliverable Summary

## *Supported Directories*

This release supports password synchronization for the following directory types, out of the box:

- Monitor Password Change: Active Directory
- Set Updated Password: Active Directory, Office 365

## *Features and Functionality*

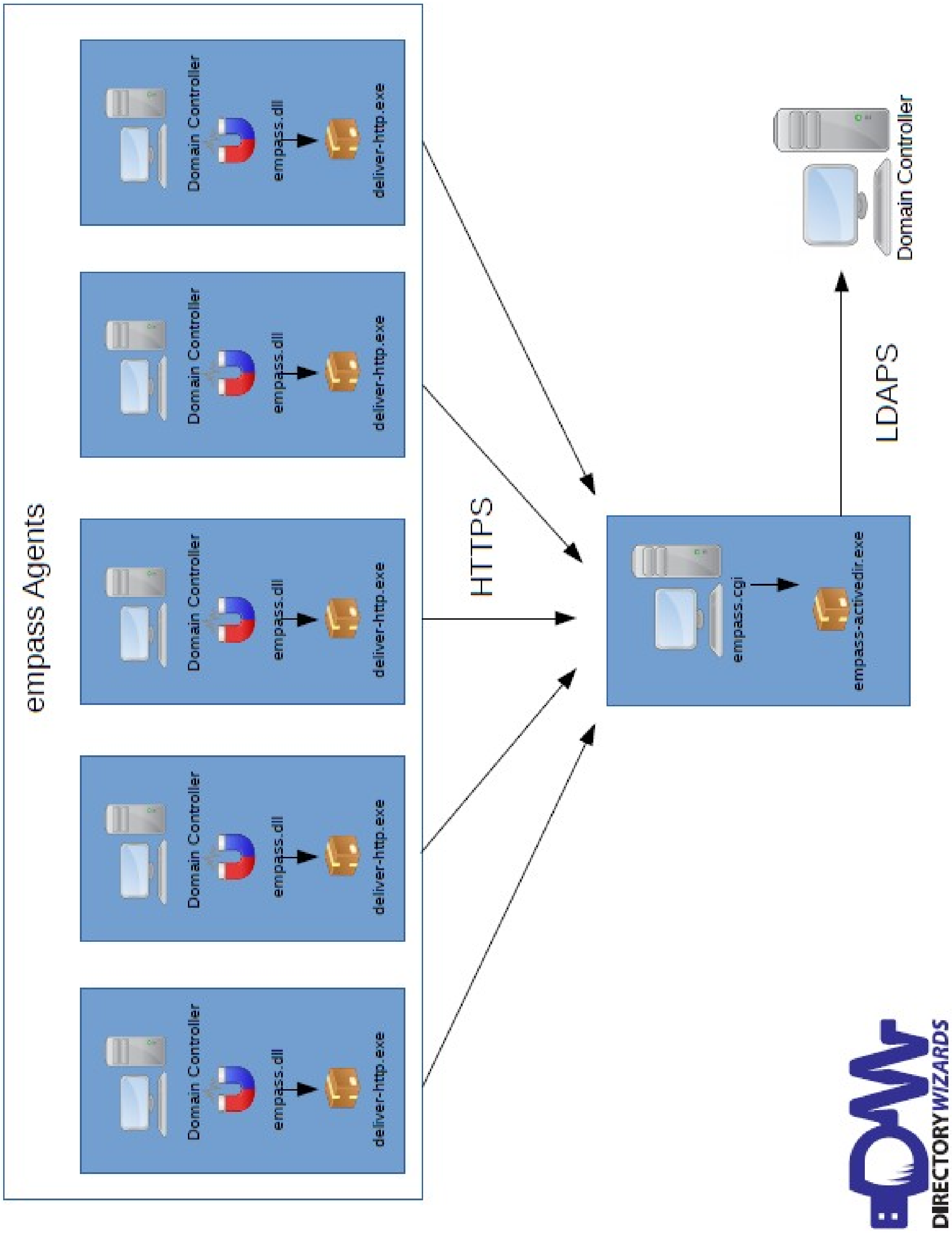
- Prompt detection of password changes via Agent(s)
- Prompt update of passwords across domains
- Live heartbeat monitoring from Agent(s) to Central Server
- Agent and Central Server queues to ensure accuracy and dependability
- AES256 encryption support (transport)
- RSA public/private key (4096 bits) encryption support (storage)
- HTTPS and LDAPS support (transport)
- Eventlog and syslog support for application monitoring

# Fixes and Enhancements

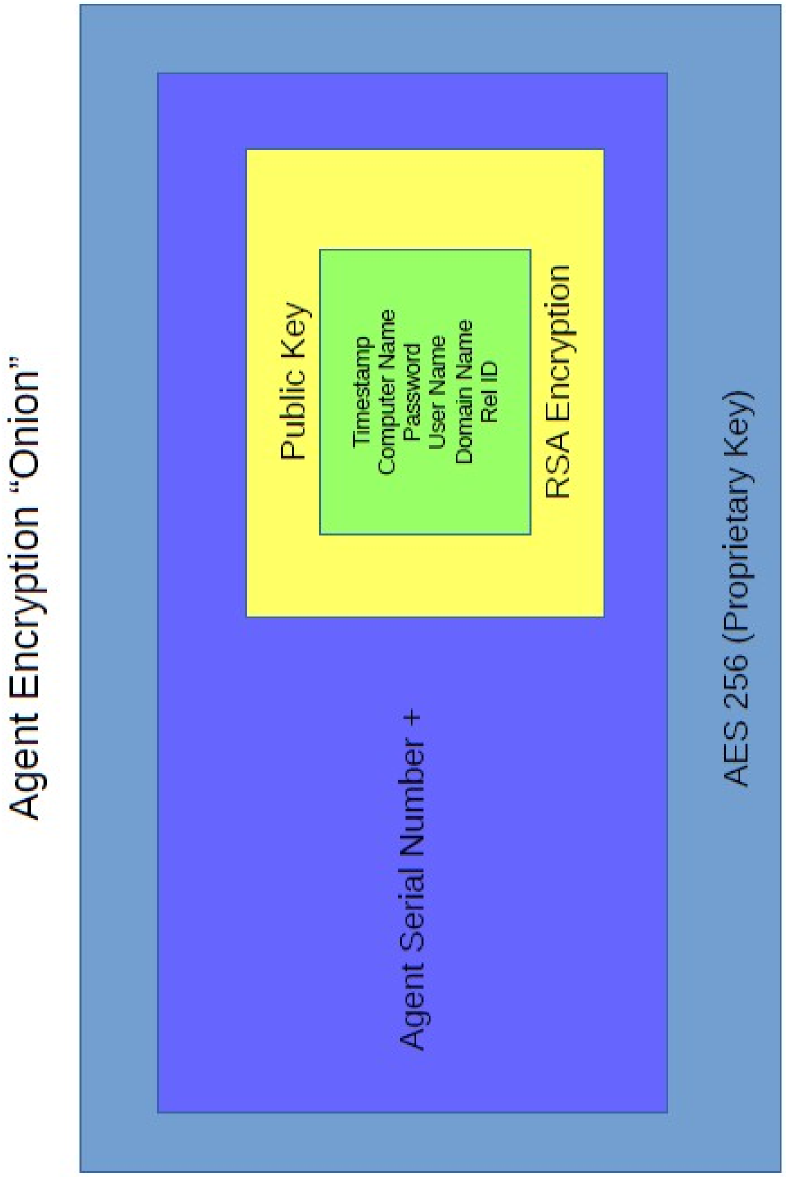
## *emPass v2.0  (and minor 1.x versions)*

- Add: emPass Agent Heartbeat.  Once the Agent is up and running, there is a real time heartbeat between Agent(s) and Central Server. This allows for monitoring of connectivity and operation between the Agent(s) and the Central Server.
- Add: Improved Agent and Central Server Queues to help maintain accuracy.   to cover brief downtimes of Central Server or loss of contact with target domain.

# Appendix 1: Diagram of typical emPass installation



# Appendix 2: Diagram of emPass encryption


Agent Encryption "Onion"
AES 256 (Proprietary Key)
Agent Serial Number +
Public Key
RSA Encryption
Timestamp
Computer Name
Password
User Name
Domain Name
Rel ID