VigiLanz Connect Cerner Instructions

VigiLanz Corporation

November 2019

Table of Contents

Cerner Services Setup Overview

A technical guide to getting Cerner Services installed and operational on a single server. This is intended for technical resources familiar with Cerner and CCL/MPages.
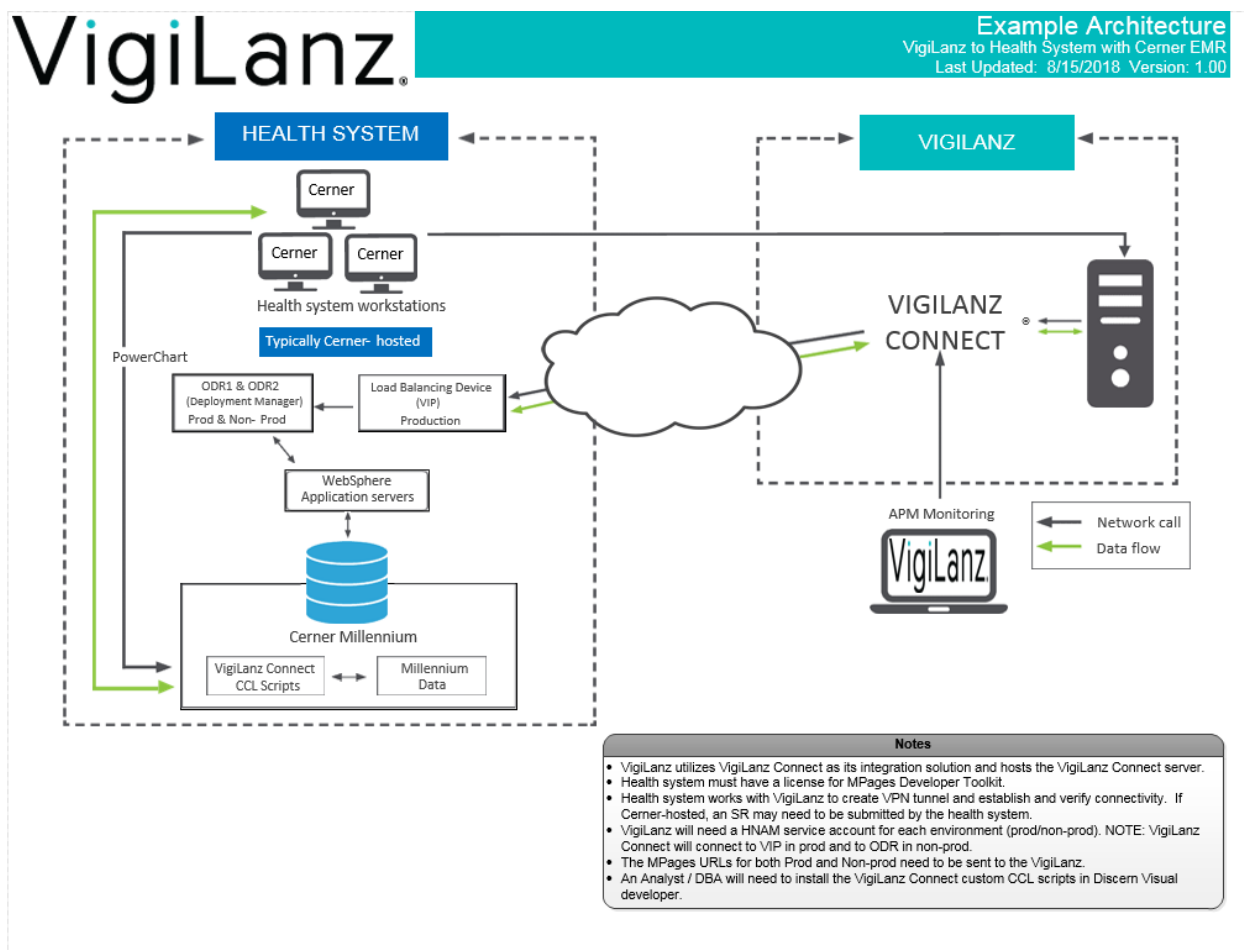
Please verify with CernerWorks if your site is Cerner hosted or with your site's Cerner CCL/MPages technical leader to ensure the following pre-requisites within this Install Instruction guide have been met prior to proceeding.

Installation Guide Information includes:
1) Architecture Diagram
2) Account access,
3) Installation.

Architecture Diagram

The integration solution consists of the digital health partner's application making a request to the VigiLanz Connect middleware server which in turn calls the Health System's ODR or Load Balancing Device which then calls the WebSphere Application Servers along with the VigiLanz Connect CCL Scripts. The below diagram is an example of the architecture:

Example Architecture
VigiLanz to Health System with Cerner EMR
Last Updated: 8/15/2018 Version: 1.00

Notes
- VigiLanz utilizes VigiLanz Connect as its integration solution and hosts the VigiLanz Connect server.
- Health system must have a license for MPages Developer Toolkit.
- Health system works with VigiLanz to create VPN tunnel and establish and verify connectivity. If Cerner-hosted, an SR may need to be submitted by the health system.
- VigiLanz will need a HNAM service account for each environment (prod/non-prod). NOTE: VigiLanz Connect will connect to VIP in prod and to ODR in non-prod.
- The MPages URLs for both Prod and Non-prod need to be sent to the VigiLanz.
- An Analyst / DBA will need to install the VigiLanz Connect custom CCL scripts in Discern Visual developer.

Before Getting Started

Before getting started, please review the bullets below to ensure the following Cerner package, Licenses, Servers and Environments are in place and ready for VigiLanz Connect installation:

✓ Confirm Cerner package 87399 (or its equivalent) is already installed.
✓ Proper license to MPages development Toolkit (PS-22700).
✓ Install & Deploy Discern Web Services on a non-production and production WebSphere application server.
  • The Discern MPages URLs must be provided to VigiLanz. This would be an example:
    http://<IP of VIP or ODR server>/discern/<domain>.<site_mnemonic>.cernerasp.com/mpages/reports
✓ Ensure the person (typically a Cerner Millennium analyst) that will perform the installation has DBA access (or equivalent approved role).
  • The Cerner Millennium analyst must have the ability to include CCL programs with GROUP0 in Discern Visual Developer (front-end accounts for GROUP0) or backend CCL.

Environment Considerations (Non-Production / Production)
It is recommended that customers set up standard non-production environment separate from the production environment for the purposes of testing prior to going live in production.

User Access and Accounts
To provide full support for VigiLanz Connect and underlying CCL programs, the following access is required:

> NOTE: If account request forms are required, please send them to the implementation project manager at VigiLanz.

1. **HNAM User Account:** Create new HNAM User Account with a position code (e.g. IT Analyst, Support Analyst, etc.) appropriate for non-production and production support access to Millennium® applications.

| Account Type	Environment(s)	Purpose
The following HNAM User Account setup is required for any 3rd party to authenticate and authorize CCL programs through Cerner Discern Web services: 1) TaskAccess.exe 2) CoreCodeBuilder.exe 3) HNAUser.exe **Note**: These steps are only required for 3rd party systems that will not pass along named user accounts for users already built within HNAUser. Please follow the steps below to set up the HNAM User Account.	- Non-Production - Production	Testing and Support

Account Steps:

1. **TaskAccess.exe**
   a) Create a new Application Group:
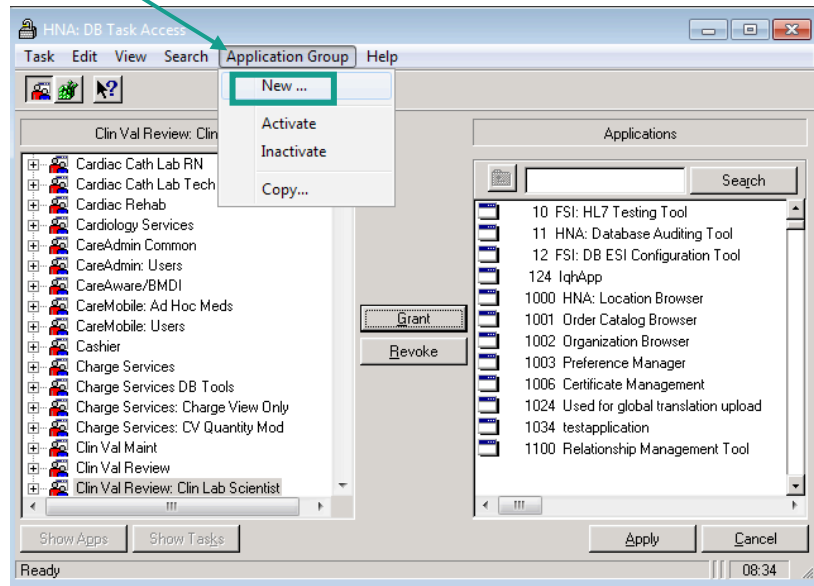
   b) Name the new Application Group: "Emissary App" (if it doesn't already exist), click "OK":
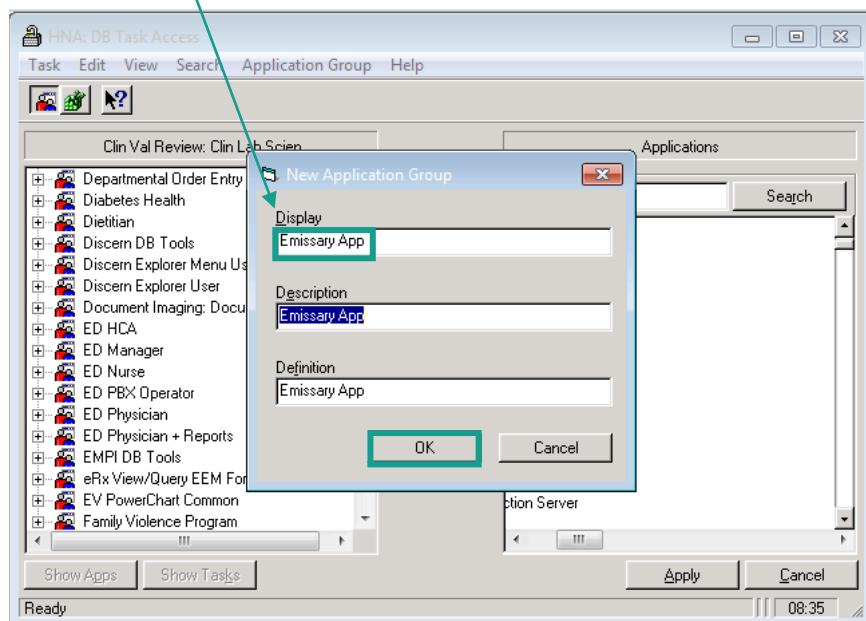
c) For the **Emissary App**, click "Grant" and the Task Access box will pop up. Then, click "Yes" to Grant ALL Tasks Associated with Application(s):
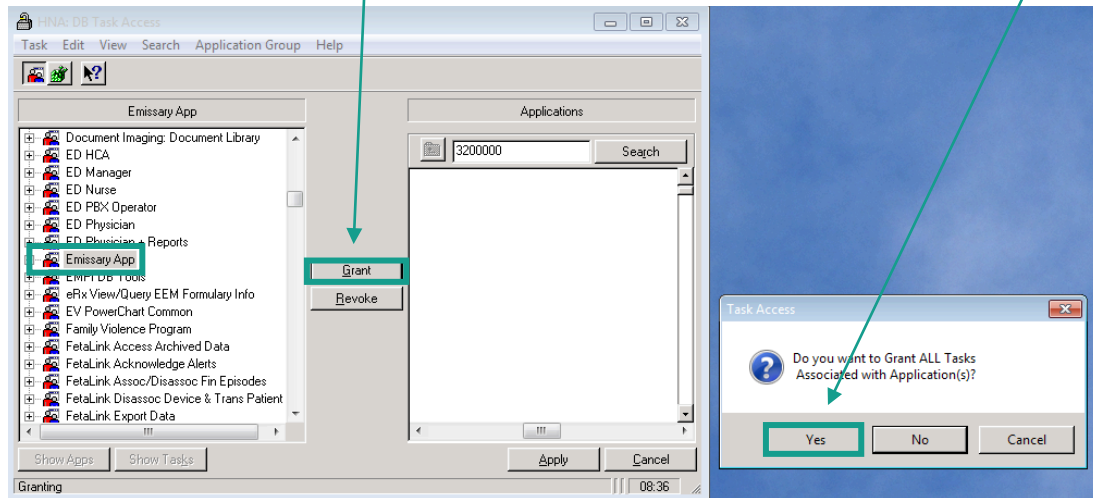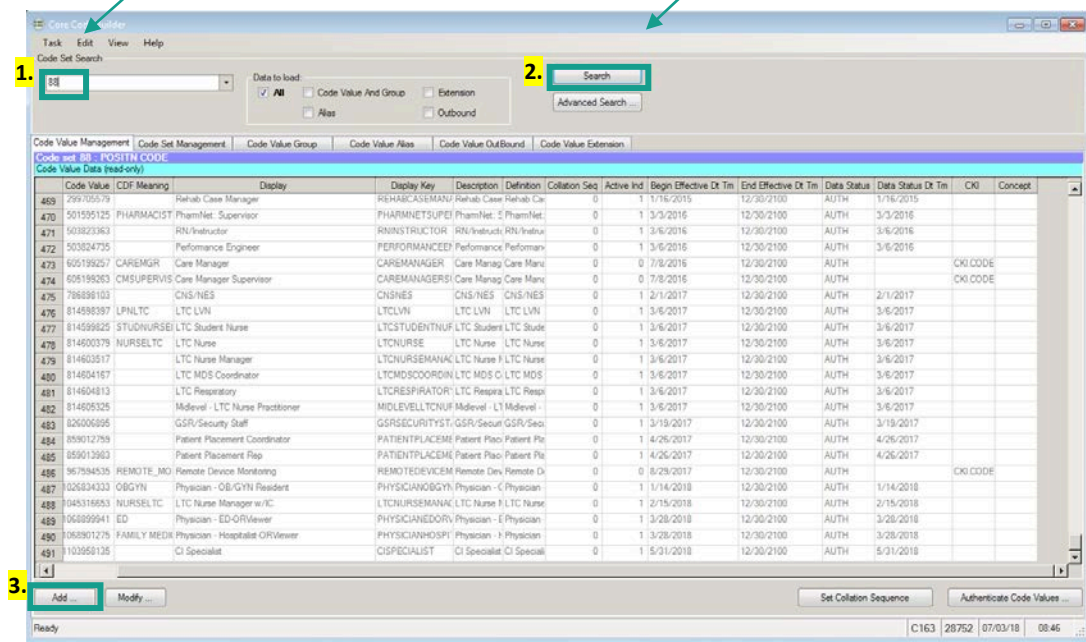

d) For the **Emissary App, 320000**, click "Grant" and the Task Access box will pop up. Click "Yes" to Grant ALL Tasks Associated with Application(s):
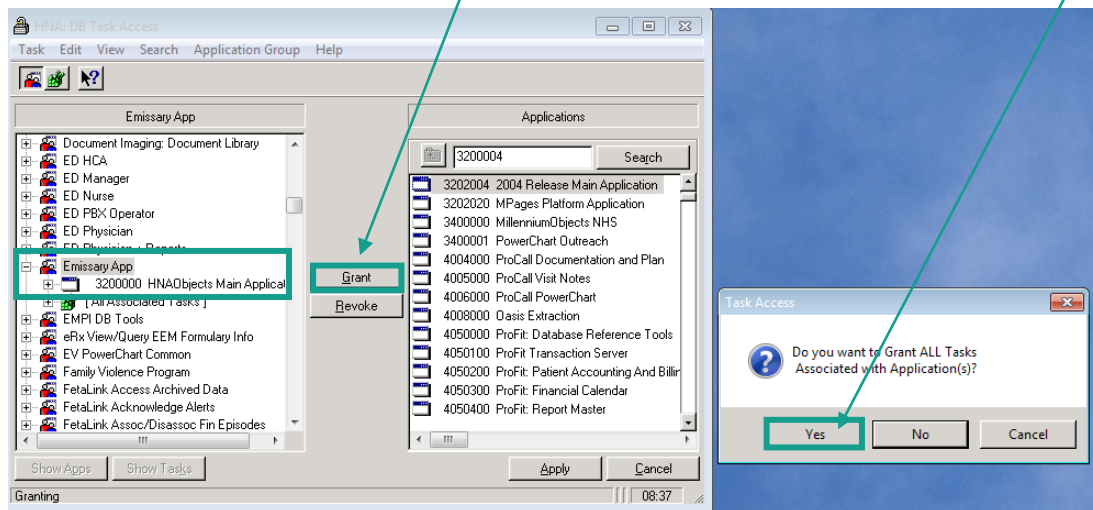
2. **CoreCodeBuilder.exe**

a) Open the "CoreCodeBuilder.exe":
Then, enter "88" in the "Code Set Search" text box, click Search. Search for the "Emissary Integration" in the Display Field. If it doesn't already exist, click the "Add" button:

b) In the "Code Set 88 : POSITN CODE", create a Display and Description of "Emissary Integration" then click "Ok":
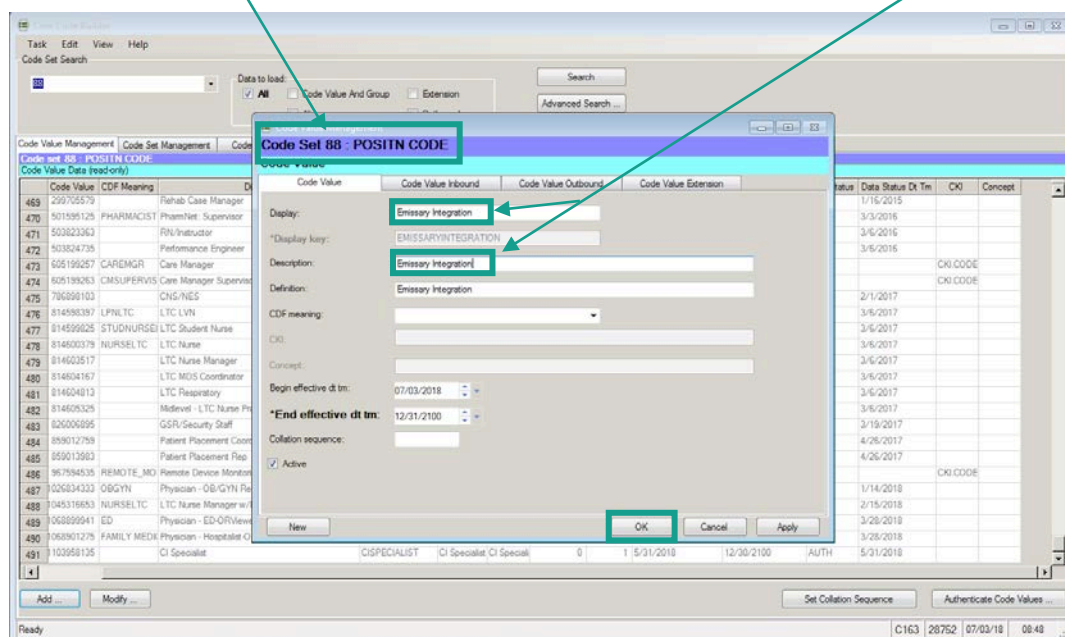
3. **HNAUser.exe**:

a) Create a new 3rd party user for the application that will integrate through Emissary:
In the "User Maintenance" window Task in the Toolbar, select "Maintain" and then "Positions":
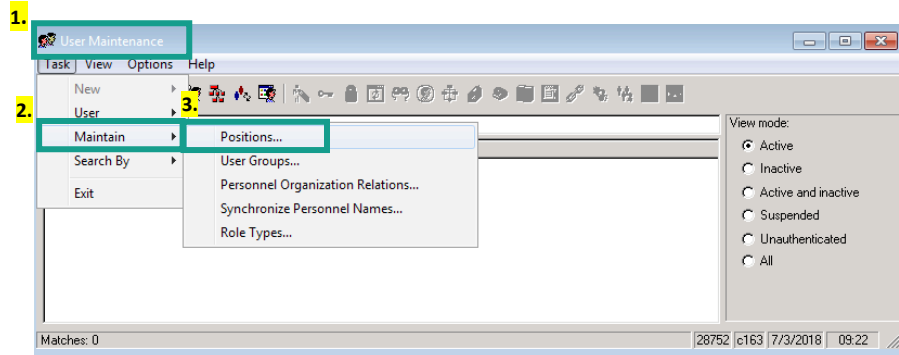
b) In the "Maintain Positions" Window, select the position "Emissary Integration" from the Position drop-down menu:
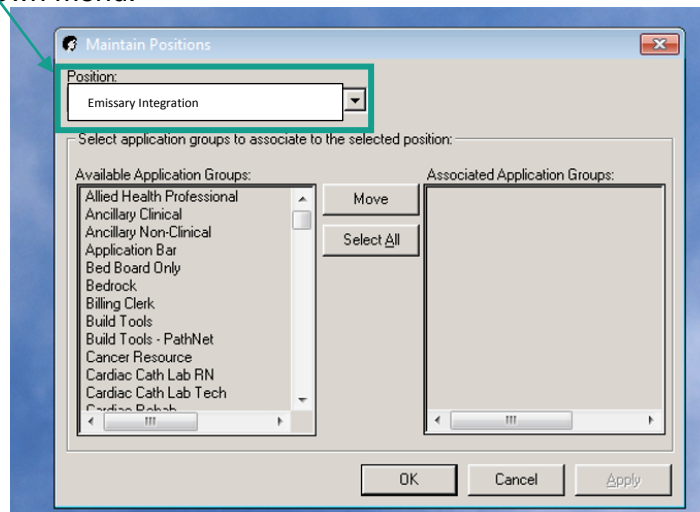
c) In the "Available Application Groups" window, click the "Emissary App" and "Move" to the "Associated Application Groups", then click "Ok":
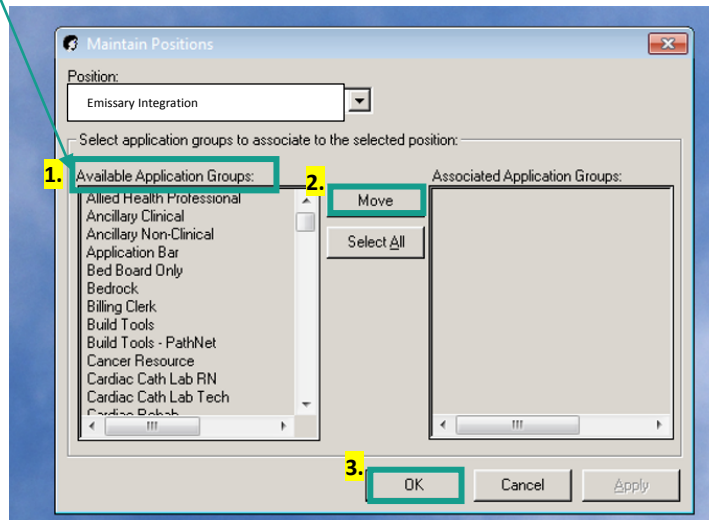
d) <u>Add a new User with the following characteristics:</u>
- Username: vigilanz
- Last Name: VigiLanz
- First Name: SYSTEM
- Position: Emissary Integration
- Password: (coordinate and share only with 3rd party personnel)
- Privileges: Un-Check most (if not all) of the privileges listed. This will restrict any domain-level privileges unnecessary for the system account.
- <u>Restrictions</u>:
  - ✓ Check: Password may not be changed in privileges/restrictions
  - ✓ Un-Check: Pre-expire password anytime password is set in HNAUser
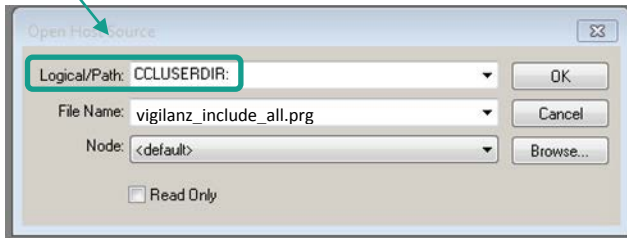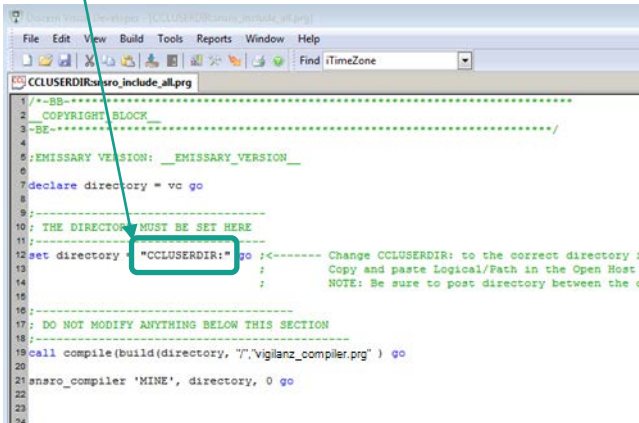
Installation

CCL Installation and Updates:

Installation and updates are typically performed by a CCL developer/analyst, but may hold a different title or role depending on organization. The individual performing the installation must have access to copy the files specified below to either the CCLUSERDIR or custom directory. The following steps in pages 12 and 13 will provide the CCL script inclusion process for the VigiLanz Connect application.

Note: For subsequent release updates, there is no need to delete anything before installing the updated CCL scripts.

Install Steps

Step	Action
1	Unzip the emr_cerner.zip file provided to you and import all the files (*.prg) in an appropriate directory on the backend (e.g. CCLUSERDIR: or some other custom directory like CUST_SCRIPT:).
2	At the CCL prompt on the backend, or in DVDEV development environment, open the CCLUSERDIR:vigilanz_include_all.prg program (Note: the screenshot below is for DVDEV). Change the directory to match the "Logical/Path" selected in Step 1 above:

3	Compile (CTRL+F7), this program will compile all vigilanz CCL programs used by VigiLanz Connect on all nodes.

NOTE: In the Output window in DVDEV, make sure all nodes appear for compiling to ensure the CCL programs were installed on all nodes. If you do not see all nodes in the Output window, compile again until you see all nodes listed in the Output window.
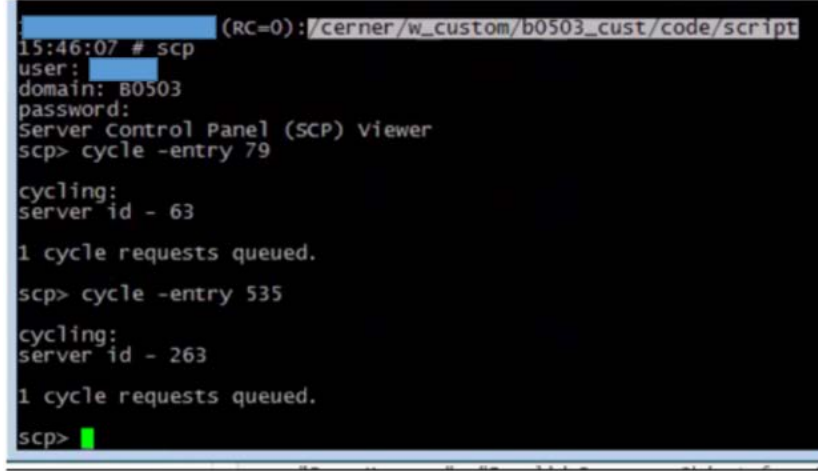
4	After compiling, click on the "List" icon. Review the "Status" and ensure all have a "Success" response with "0 error(s)":

5	Cycle (stop and start) all associated MPages servers 79, 178 (if applicable), 179 (if applicable), and 535 on all nodes.
6	Test the VigiLanz Connect GET Versions API call. Once the servers are back online, ensure the dates on the payload matches the install date and the version number matches the VigiLanz Connect version.
	Only follow the steps below if the install fails.
7	If the install fails, check directory permissions and try deleting the .prg files on all nodes and then reloading. Try installation process again. If further assistance is required, please contact VigiLanz Customer Support and provide the "Error Message" that would be indicated in **Step 4** above.
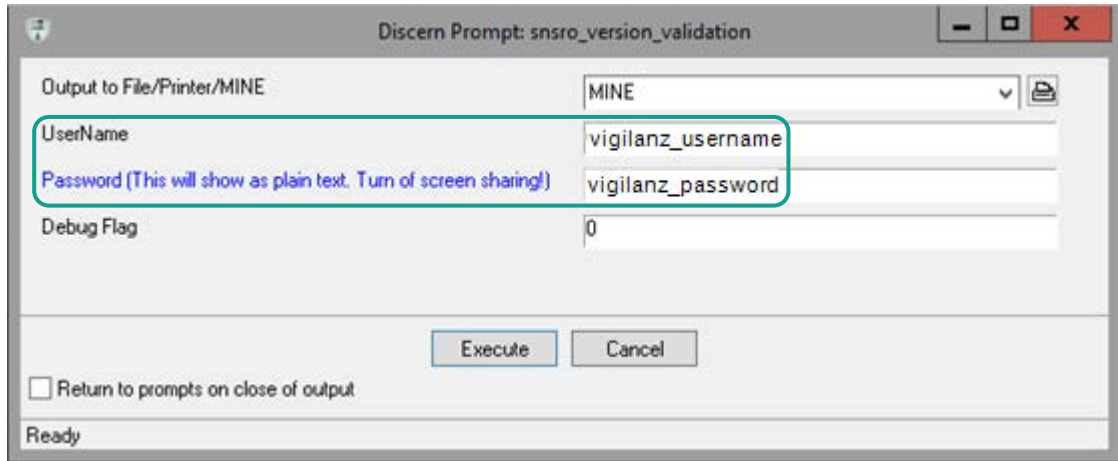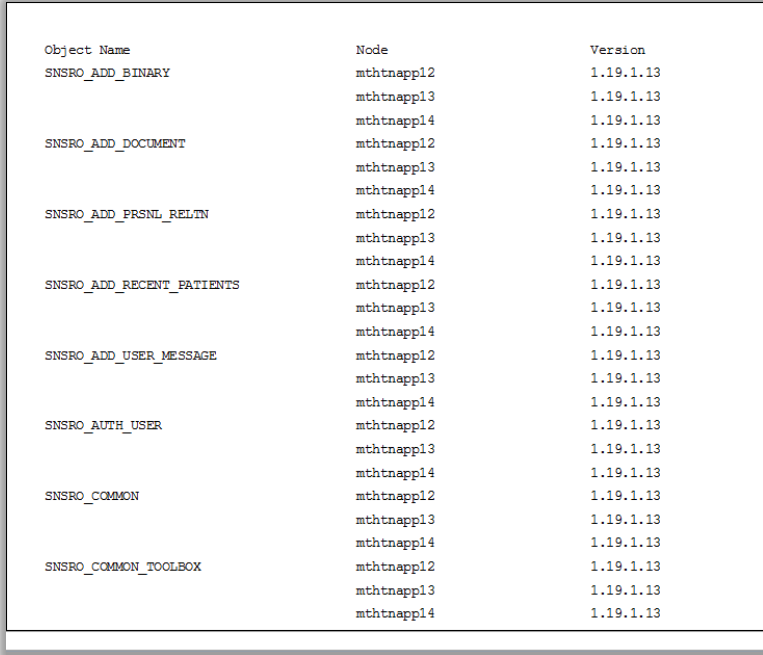
Validation

Version Validation Instructions:
After you have compiled the CCL scripts, follow these instructions to confirm that the versions match across nodes.

*Note: the file names could be prefixed differently than the examples shown in this section.

Step	Action
1	After compiling the scripts with vigilanz_include_all*, open file name: vigilanz_version_validation.prg*.

2	Click the Execute icon.
3	Enter your millennium username and password. **Important Note:** The password shows as plain text. In the event you conduct a web conference screen sharing session that includes these screens, it is recommended you turn off the screen sharing function during until you are past this screen.
4	The output will show the objects on each node and the associated versions*. The versions should match each other as well as match the version listed in the vigilanz_include_all script*. - If they match, installation across nodes is successful. - If they don't match, then the compilation across nodes failed. Continue to Step 5.
5	If the compilation failed, then delete all snsro scripts on each node and start the process over.

Subsequent CCL Update Installation

Each time a new VigiLanz Connect Release Update package is sent, the most recent version of these instructions will be included. Follow the same steps as the initial installation instruction to overwrite the necessary files. There is no need to delete anything before installing the updated CCL Files.

Important Note: Prior to updating the latest Release, please confirm with your VigiLanz Connect Server Hosting Organization they have updated their VigiLanz Connect Middleware with the latest version.