Centralized Installer and ICMS Framework Installation

Installation Guide

Emerge version 3.1

Landis+Gyr

Limitation on Warranties and Liability

Contact Us:

To provide feedback about this document, email us at ustechnicaldocumentation@landisgyr.com

Customer Support: 1-888-390-5733 | support.na@landisgyr.com

98-3200 Rev AD | Emerge Installation Using the Centralized Installer and ICMS Framework | November 13, 2024

Table of Contents

Revision History

Summary of Changes

Rev	Version	Change Summary
AD	3.1	Remove Oracle Preparation and Oracle Summery Sheet from Chapter 2 of the document and migrated it to the Main Installation Guide.
AC	2.2	Updated the title as Emerge 3.1 Centralized Installer and ICMS Framework Installation Guide and removed Package Versions from the cover page.
		Updated special characters exclusion list for database passwords. See "Database Passwords" on page 2-19.
		Added a note to the CIN Server Preparation section regarding sa account password usage. See "SQL Database Preparation for ICMS" on page 24.
		Removed instances of value "HTTP" from the document.
		Removed "Specific Emerge Versions" section from chapter 5.
		Minor formatting and editing updates. No feature/functionality changes.
AB	2.1	Updated it as Emerge 2.1 Installation Using the Centralized Installer and ICMS Framework Installation Guide.
AA	2.0	Created it as Emerge 2.0 Installation Using the Centralized Installer and ICMS Framework Installation Guide.

1
Introduction

Background

Landis+Gyr is introducing the Centralized Installer (CIN) platform and its Installation and Configuration Management Service (ICMS) framework, as a highly scalable innovative way of deploying its product line while using very little access to servers and reducing the required maintenance window for an upgrade from hours to minutes irrespective of the number of servers.

The core of the CIN is driven by the ICMS service, that maintains a database of all available packages and configuration settings tailored for every Organization managed by the CIN platform. The ICMS and its database content is accessible through a user interface (CINUI) where operators prepare Organizations configuration and orchestrate their deployment to servers. Each server member of an Organization will have an Installation Agent Service (IAS) connected to the ICMS and accepting all commands and customized packages for preparation and installation of the components.

Figure 1 - 1 summarizes the main components of the Centralized Installer platform and ICMS framework.
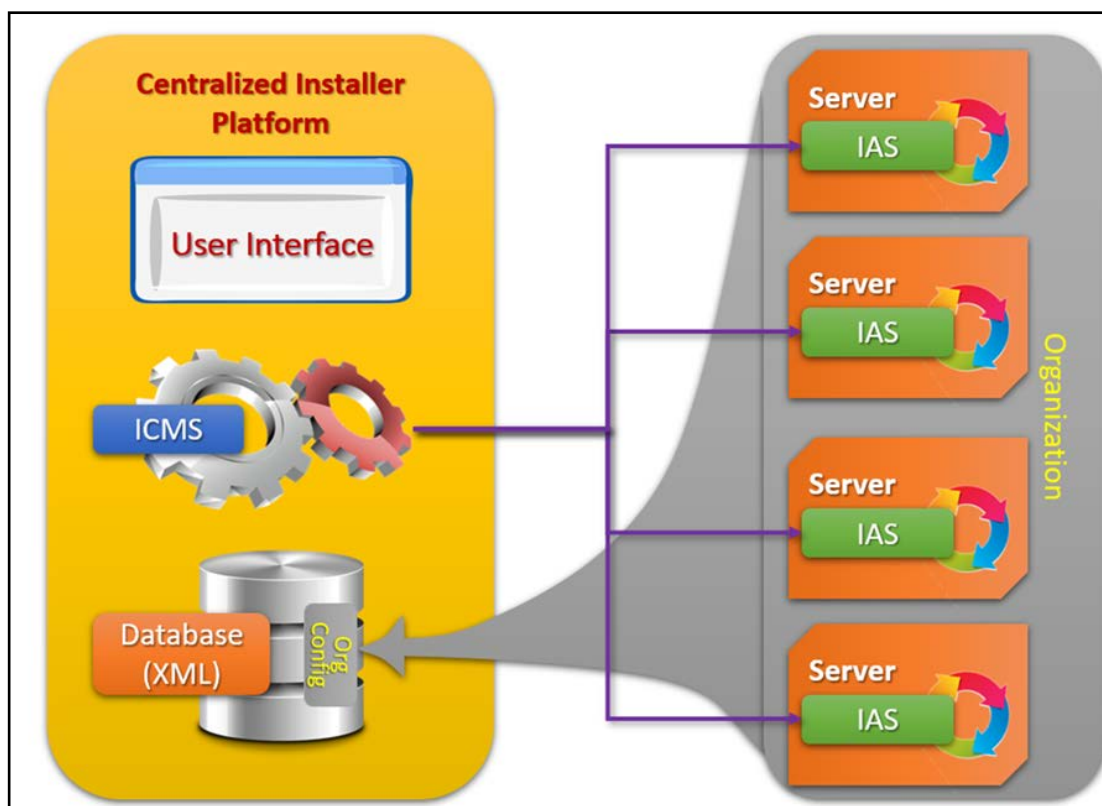
Figure 1 - 1. Centralized Installer Platform

Definitions

The following keywords are used through this document, to facilitate reading.

Table 1 - 1. Definitions

Component	Role/Definition
HES	Head-end system or Emerge.
ICMS	Installation and Configuration Management Service - core service registered as a Windows Service, that handles the entire remote installation framework. This service maintains an XML database of all organizations and settings required to perform installation and maintenance tasks on Landis+Gyr products that support **ICMS** installation.
CIN-UI	Centralized Installer User Interface - web-based GUI allowing easy configuration and operation of the **ICMS** service.
IAS	Installation Agent Service - software component residing on all Landis+Gyr servers allowing remote installation of any components through the **ICMS** framework.
CIN	Designate a dedicated platform/server where **ICMS** and **CIN-UI** components are installed.
Organization	In the context of an ICMS-based installation, an organization represents a specific environment being managed by the **ICMS** framework. This friendly name must be unique to the current ICMS platform.
Instance	In the context of an ICMS-based installation, an instance is a unique identifier associated to an **Organization**, but because it is used programmatically it cannot contain spaces nor special characters. It must be unique to the current **ICMS** platform.
Profile	In **ICMS** context, a **Profile** is the sum of all components from any number of ICMS packages that would be assigned to a specific server tier, irrespective of number of servers part of this tier. A **Profile** is the **ICMS** representation of the *role* that any server tier plays in an Organization.

ICMS Installation Add-On Documents

This guide presents the general information required for a successful Emerge installation but details specific to each component part of the HES installation are NOT included in this guide. A series of companion documents called **ICMS Installation Add-Ons** are published with every Emerge release and contain every detail relative to the ICMS package it represents. Do not start any **ICMS**-based installation without obtaining and reading the **ICMS Installation Add-On** document for each package being used.

Table 1 - 2. Available Add-On Documents

Number	Document Name
98-2270	ICMS Installation Add-On: ANSI Adapter Package Specifics
98-2273	ICMS Installation Add-On: Integration Suite Package Specifics
98-2274	ICMS Installation Add-On: Key Manager Package Specifics
98-2275	ICMS Installation Add-On: RF Mesh IP Adapter Package Specifics
98-2287	ICMS Installation Add-On: Low Energy Network Adapter Specifics
98-2288	ICMS Installation Add-On: Low Energy Meter Adapter Specifics
98-2289	ICMS Installation Add-On: Platform GND Converter Package Specifics
98-2291	ICMS Installation Add-On: Device Hub Installation Specifics

Table 1 - 2. Available Add-On Documents

Number	Document Name
98-2305	ICMS Installation Add-On: Kafka and Zookeeper Package Specifics
98-2307	ICMS Installation Add-On: M2M Installation Package Specifics
98-2353	ICMS Installation Add-On: Tunnel Manager Package Specifics
98-2375	ICMS Installation Add-On: Application Manager Package Specifics
98-2491	ICMS Installation Add-On: PANA Service Package Specifics
98-2515	ICMS Installation Add-On: Platform DLMS Device Driver Service Package Specifics
98-2516	ICMS Installation Add-On: COSEM Service Package Specifics
98-2517	ICMS Installation Add-On: Gulf Import Service Package Specifics
98-2518	ICMS Installation Add-On: LTE Adapter Package Specifics
98-2519	ICMS Installation Add-On: PSTN Adapter Package Specifics
98-2548	ICMS Installation Add-On: Store and Forward Service Package Specifics
98-2570	ICMS Installation Add-On: Gemalto Luna Client Package Specifics Package Specifics
98-2622	ICMS Installation Add-On: Data Streaming Package Specifics
98-2810	ICMS Installation Add-On: Performance Monitoring Dashboards Package Specifics
98-2823	ICMS Installation Add-On: IP Gateway Package Specifics
98-2952	ICMS Installation Add-On: IoT Gateway Package Specifics
98-2973	ICMS Installation Add-On: RadiusServer for Wi-SUN Package Specifics
98-2976	ICMS Installation Add-On: FND Adapter Package Specifics
98-2977	ICMS Installation Add-On: Wi-SUN Adapter Package Specifics
98-2980	ICMS Installation Add-On: Firmware Differential Image Generator Service Package Specifics

2
Prerequisites for Installation

Server Networking Preparation

This section presents the fundamentals of server networking preparation for a complete Emerge deployment.

Typical Network Connectivity

The diagram below presents a high-level view of the proposed network connectivity of all components. It is understood that each system in the data center can be designed according to this scheme, and network connecting the User Domain with the Server Domain can enforce security on communications through a firewall or other security appliances.
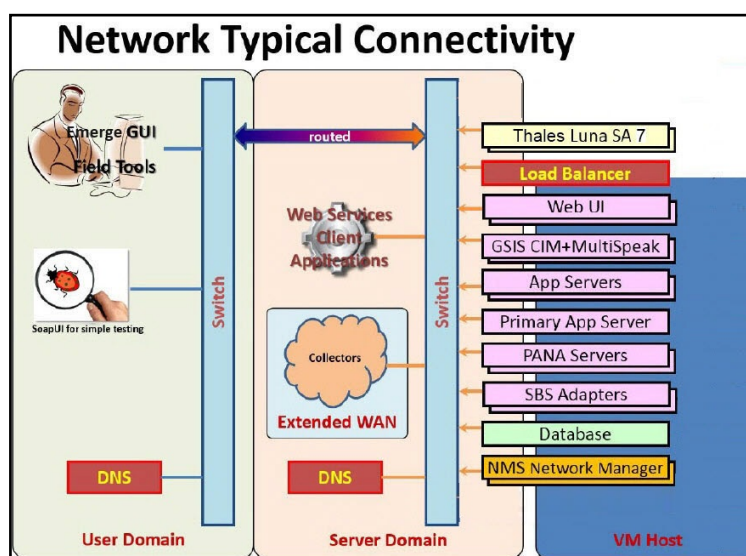
Figure 2 - 1. Typical Network Connectivity

- **User Domain**. The User Domain, when using Active Directory to manage user accounts and access to resources, is the typical domain where these users will be hosted. Some customer implementations will have multiple domains segmented for different user classifications. User workstations may also be part of this domain.

- **Server Domain**. The Server Domain, when using Active Directory to manage server accounts and user access, is the typical domain where these servers will be hosted. In most cases, multiple Organizational Units (OUs) will be configured and Group Policy Objects (GPOs) can be applied to each OU individually, thus easing servers' management.

ⓘ **NOTE:** Customers not experienced in managing OUs and GPOs should not attempt this in the context of a Emerge deployment.

It is possible to use a single domain to manage users, workstations, and servers, and make exhaustive use of OUs and GPOs to enforce various security restrictions. This is purely customer-dependent.

- **VM Host**. Multiple vendors provide hypervisors that, when installed on a usually very powerful server, become a *VM Host* where resources are shared amongst multiple virtual machines. Some well-known vendors in the marketplace today are Microsoft (Hyper-V) and vmware (ESXi).

Extended WAN

This is the data-center zone where the **Extended WAN** will deliver data flows from field components to the data-center. Landis+Gyr recommends using an appliance in this zone to route traffic from collectors to a more secure data-center zone where application servers will be located.

Active Directory Specifics

If the customer implementation uses Active Directory to manage user access to Emerge and other resources, it is required to implement a two-way trust between User domain and Server domain, where client users and the HES servers reside. This is only applicable if both User and Server domains are different.

In addition, under this very specific condition, it will be required to use **Universal** security groups in order to allow information to be published properly in Emerge.

Network Interface Cards on Servers

Windows Server NIC Preparation

Some important aspects to look for:

1. On all NICs, good practice dictates to remove bindings to all unnecessary protocols (QoS Packet Scheduler, Link-Layer Topology, etc…).

   a. Keep Client for Microsoft, File and Printer Sharing, and IPv4.

   b. Keep IPv6 on a NIC only if/where required.

NMS Servers, `eth0` would be collector-facing and `eth1` would be RF Mesh IP-facing.

Linux Tunnel Manager NIC Preparation

For **RF Mesh IP** deployments, **Tunnel Manager** server will most possibly require IPv4 and IPv6 addressing.

If this is accomplished using dual-NIC configuration, interface **ens192/eth0** would be collector-facing and interface **ens224/eth1** would be RF Mesh IP-facing.

Server Hosted Firewall

Current version of Landis+Gyr installation scripts do not handle auto-configuration of built-in server firewalls. On all servers (Windows and Linux) where Landis+Gyr components will be installed, disable any built-in firewalls for proper operation.

URLs and DNS Preparation

Service Names Definitions

The following table must be updated to fit the environment being built. References are made to these entries in all relevant locations throughout the installation steps. It is good practice and very convenient to use **Service Names** instead of the actual server names for all of these entries, it allows for easier configuration and later modifications without re-installation of any components. Each Environment-specific DNS entry will refer to an actual server in some cases, or to a VIP associated to a Load Balancer port in others. Landis+Gyr recommends that a **Service Name** DNS entry be created for each of the following pseudonyms presented in Table 2 - 1.

Table 2 - 1. Service URL Definitions

Pseudonym in install guides	Environment-specific DNS	IP address
Emerge-WebUI		
DB-Service		
Inbound-to-EmergeApp		
Inbound-to-EmergePri		
RFMesh-to-NetMgr		
Inbound-to-EmergeApp		
Inbound-to-ISMH		
External-to-ISCIM		
External-to-ISMS		
RFMeshIP-to-SBS		
RFMeshIP-to-PANA		
Inbound-to-MeshIP		
CellMeters-to-NetMgr		
Inbound-to-M2M		
Inbound-to-RFA		
Inbound-to-WiSUN		

DNS Preparation

In the above table, every entry must have a matching record in DNS.

Pseudonyms Definitions

The table below presents information and instructions pertaining to each pseudonym.

Table 2 - 2. Pseudonyms Definitions

Pseudonym	Definition/Usage
Emerge-WebUI	This is used to access the Landis+Gyr Emerge web server, by interactive users for Emerge interface, or from field tools for authentication. When Emerge has a single web server, this DNS entry can resolve to the Emerge Web server itself. When multiple Emerge web servers are used, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all Emerge Web servers. The _ character cannot be used as part of the DNS entry for the Emerge web page access.
DB-Service	DNS entry resolving to the Emerge primary database server, or to a VIP representing a cluster of database servers. This will vary according to the custom database implementation. It is not recommended to use the server DNS entry itself in the product configuration; should the database hostname ever changes for any reason, the Emerge would have to be stopped and reconfigured. It is not recommended to route database data connections through any appliance, due to the large volume of transactions.
Inbound-to-EmergePri	DNS entry resolving to the Emerge Primary Application Server only, used by Emerge web servers to interact with features served by the Primary Application Server only.
RFMesh-to-NetMgr	DNS entry resolving to Emerge Application servers, used by Gridstream-RF collectors to communicate with the application server of the Emerge. When only one Application server is installed, this DNS entry can resolve to the Application server itself. When two or more Application servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all Application Servers.
Inbound-to-EmergeApp	DNS entry resolving to Emerge Application servers, used by any Emerge server tier as well as adapter layer (M2M and RF Mesh IP) to communicate with the application layer of the Emerge. When only one Application server is installed, this DNS entry can resolve to the Application server itself. When two or more Application servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all Application Servers.
Inbound-to-ISMH	DNS entry resolving to Gridstream Integration Suite Server hosting Message Handlers, used by every server of the Emerge (Web, Primary and Application) to send various messages (such as events and commands asynchronous responses) to the Gridstream Integration Suite integration layer destined to external system. Not required when Gridstream Integration Suite is not being used. When only one Gridstream Integration Suite server is installed, this DNS entry can resolve to the Gridstream Integration Suite server itself. When two or more Gridstream Integration Suite servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all Gridstream Integration Suite servers.
External-to-ISCIM	DNS entry used on MDM or other external systems to access the Gridstream Integration Suite Server hosting Message Handlers integration layer to send CIM commands. Not required when Gridstream Integration Suite is not being used. When only one Gridstream Integration Suite server is installed, this DNS entry can resolve to the Gridstream Integration Suite server itself. When multiple Gridstream Integration Suite servers are used, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all Gridstream Integration Suite servers.
External-to-ISMS	DNS entry used on MDM or other external systems to access the MultiSpeak web services. Not required when MultiSpeak is not being used. MultiSpeak is typically installed as part of the Emerge Web server, but the component can also be installed manually on Gridstream Integration Suite servers if desired. When only one MultiSpeak server is installed, this DNS entry can resolve to the MultiSpeak server itself. When multiple MultiSpeak servers are used, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all MultiSpeak servers.

Table 2 - 2. Pseudonyms Definitions (Continued)

Pseudonym	Definition/Usage
NMS-Inbound	DNS entry used for inbound **initial** connections requests from all RF Mesh IP endpoints will resolve to NMS servers. This can be used by the backhaul Carrier, or on endpoint themselves according to the network configuration. Not required when RF Mesh IP endpoints are not being used. When only one NMS server is installed, this DNS entry can resolve to the NMS server itself. When two or more NMS servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all NMS servers.
RFMeshIP-to-SBS	DNS entry resolving to RF Mesh IP servers IPv6, used by RF Mesh IP endpoints to communicate with RF Mesh IP servers through NMS servers. Not required when RF Mesh IP endpoints are not being used. Required only when using a native IPv6 network between NMS and RF Mesh IP. When only one RF Mesh IP server is installed, this DNS entry can resolve to the RF Mesh IP server itself. When two or more RF Mesh IP servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all RF Mesh IP servers.
RFMeshIP-to-PANA	DNS entry resolving to PANA servers IPv6 address, used by endpoints to communicate with PANA servers through NMS servers. Not required when RF Mesh IP endpoints are not being used. Required only when using a native IPv6 network between NMS and PANA. When only one PANA server is installed, this DNS entry can resolve to the PANA server itself. When two or more PANA servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all PANA servers.
Inbound-to-MeshIP	DNS entry resolving to RF Mesh IP servers, used by Emerge Application Servers to communicate with RF Mesh IP servers to send message to RF Mesh IP endpoints. Not required when RF Mesh IP endpoints are not being used. When only one RF Mesh IP server is installed, this DNS entry can resolve to the RF Mesh IP server itself. When two or more RF Mesh IP servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all RF Mesh IP Servers.
CellMeters-to-NetMgr	DNS entry used for inbound connections from Enhanced Cellular modems, will resolve to M2M Servers. This can be used by the Cellular Carrier, or on endpoint themselves according to the network configuration. Not required when Enhanced Cellular / M2M endpoints are not being used. When only one M2M server is installed, this DNS entry can resolve to the M2M server itself. When two or more M2M servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all M2M servers.
Inbound-to-M2M	DNS entry resolving to M2M servers, used by Emerge Application Servers to communicate with M2M servers to send message to Enhanced Cellular endpoints. Not required when Enhanced Cellular / M2M endpoints are not being used - use the Application Server FQDN in this case during the installation process, or use **Inbound-to-EmergeApp** FQDN when installing on a Web server. When only one M2M server is installed, this DNS entry can resolve to the M2M server itself. When two or more M2M servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all M2M Servers.
Inbound-to-RFA	DNS entry resolving to RF Application servers, used by Emerge Application Servers. Follow Landis+Gyr recommendations for this value - use the Application server FQDN by default during the installation process, or use **Inbound-to-EmergeApp** FQDN when installing on a Web server.
Inbound-to-WiSUN	DNS entry resolving to WiSUN servers, used by Emerge Application Servers to communicate with WiSUN servers to send message to WiSUN endpoints. Not required when WiSUN endpoints are not being used. When only one WiSUN server is installed, this DNS entry can resolve to the WiSUN server itself. When two or more WiSUN servers are configured as a cluster, this DNS entry will resolve to a VIP associated to a load balancer Virtual Server representing all WiSUN Servers.

Database Preparation

Database Passwords

➡️ **IMPORTANT:** *New database accounts will be created with specified passwords during initial installation of a Package. It is **NOT** possible to change database account passwords during an upgrade using ICMS by simply changing the password in the corresponding database component settings, as the ICMS will actually validate each database account credentials against the database and any differences will cause installation of that component to fail.*

When preparing for a HES deployment, many database accounts will be created in support of the product installation. While Landis+Gyr does recommend using strong passwords, some characters must still be avoided for proper installation. It is conceivable that customers have their own special characters exclusion list, but the following are known to create problems and must not be used in any passwords for PostgreSQL, Oracle, or SQL Server accounts.

%   !   ;   '   "   /   <   @   <space>

Passwords should never start with a **$** character but **$** is supported in passwords.

In many cases customers use a more complete exclusion list of special characters:

%   ()   {}   []   <>   !&   /\   ;   ,   '   "   ?   @   <space>

It is also conceivable that some combinations of otherwise inoffensive special characters create an invalid sequence, at the moment none of these are known to Landis+Gyr.

SQL Server

Install and setup **SQL Server** on Database server.

- If using **Named Instance**, create one for the Organization.

- For each DB instance used for this Organization (default instance or named instance), enable TCP protocol and specify desired TCP port number. Restart the instance for the change to become effective.

- Emerge requires **SQL Server Authentication** mode to operate. Make sure **SQL Server** is setup to use **SQL Server and Windows Authentication mode**.

- Enable and configure Distributed Transaction Coordinator (MS DTC) by running the following command from an elevated PowerShell console (single command with multiline syntax):

```
Set-DtcNetworkSetting -InboundTransactionsEnabled $true `
-OutboundTransactionsEnabled $true `
-RemoteClientAccessEnabled $true `
-RemoteAdministrationAccessEnabled $true `
-XATransactionsEnabled $true `
-LUTransactionsEnabled $true `
-AuthenticationLevel "NoAuth"
```

SQL Server - Summary Sheet

During the installation process, the following information will be required.

Table 2 - 3. SQL Server Settings

Setting	Your Value
Database Server FQDN if using Named Instance, use **FQDN\NamedInstance** notation	
Database port	
System-like DB account - required for installation	
System-like DB account password	

Note that additional details like database names as well as application DB account credentials will be specified during the setting preparation for each component later in the installation procedure.

Final System Verifications

Idle Session Time Out

In Emerge deployments, many data flows require long-standing sessions that, if prematurely terminated by an in-path component (firewall, load balancer, etc…), will negatively impact product operations. Minimum idle session timeout values for these data flows are recommended as follows:

Table 2 - 4. Idle Session Time Out

Client web browsers to Emerge Web UI servers	30 minutes
All Emerge server(s) and database server(s)	48 hours
Emerge application server(s) and HSM security appliances	26 hours
RF Mesh Gridstream Collectors and Emerge application server(s)	35 minutes

Please make sure the above recommendations are met or exceeded.

Windows Server Checklist

⚠️ **WARNING: All servers must be built using the US-English Language and United States Region for proper product installation and operation. It is possible to apply a language pack after installation so each end user can select an alternate language presentation when performing maintenance on servers, as long as language changes remain confined to the user session and not applied system-wide.**

Basic Settings

The following Windows and Database server checklist will guide the installer in ensuring that all the required components are in place before installing Emerge:

1. Configure server(s) per Microsoft recommendations for server performance.

2. Make sure each Windows server has the following disk allocation:

   a. Dedicated drive for Landis+Gyr product installation. Suggested minimum value is 25Gbytes

   b. Dedicated Drive for MSMQ. This will greatly facilitate monitoring disk usage of MSMQ and avoid halting when reaching quotas that are much harder to monitor. As further optimization, the disk partition hosting the MSMQ drive could also reside on fast SSD physical disks to increase processing capacity of MSMQ. Suggested value is 10Gbytes, suggested drive letter **M**:

      i. Create the base `M:\MSMQ` folder.

      ii. Reconfigure **MSMQ** as follows:

         • Disable all Storage Limits.

         • Change the storage folder locations as per suggested below in respective order

            `M:\MSMQ\MessageFiles`

          M:\MSMQ\MessageLogs

            `M:\MSMQ\TransactionLogs`

         • Save Settings. MSMQ will issue a warning indicating it will restart, this is normal.

      On a new server where **MSMQ** is not installed yet, simply allocate dedicated drive and create base `M:\MSMQ` folder on it.

(i) **NOTE:** Do not create the entire folder structure other than the base `M:\MSMQ` folder, or MSMQ will fail to update its configuration.

   c. Periodically monitor `System Queues` from MSMQ subsystem. During the course of Emerge operations, some components may encounter various message delivery problems that could result in messages being routed to the `System Queues` which are usually not monitored but still consumes quota / disk space.These queues should be periodically purged since none of their messages can be reprocessed.

   Purging the `System Queues` can be accomplished from:

   `Computer Management > Services and Applications > Message Queuing > System Queues`

   ...or...

   programmatically using a simple PowerShell script adapted from the following script:

```
[Reflection.Assembly]::LoadWithPartialName("System.Messaging") | Out-Null
$Name=(get-wmiobject win32_computersystem).name
$QName=(
"FormatName:Direct=OS:$name\System$;DEADXACT",
"FormatName:Direct=OS:$name\System$;DEADLETTER"
)

foreach ($Q in $Qname)
{
    $MessageQueue = New-Object System.Messaging.MessageQueue($Q)
    $MSGCount=$($MessageQueue.GetMessageEnumerator2()).count

    if ($MSGCount)
    {
       $MessageQueue.Purge()
       Write-Host "$Q has been purged of $MSGCount messages." -ForegroundColor green
    }
    else
    {
       Write-Host "$Q is clean"
    }
}
```

➮ **IMPORTANT:** *Irrespective of the method used for monitoring and purging the* `System Queues`*, Landis+Gyr recommends purging* `System Queues` *task be scheduled for automatic execution on all servers where MSMQ will be installed in support to Landis+Gyr components.*

See Chapter 7, section **1.3 Automated Server Maintenance** *for automated MSMQ maintenance options.*

ⓘ **NOTE:** If MSMQ Journaling is ever being enabled for any reason, make sure to purge all journals since they also consume quota / disk space. Landis+Gyr components do not deploy with Journaling enabled.

    d. Consider allocating a different dedicated disk volume for memory page file. Microsoft recommends using a custom-sized page file (not system managed) of 1.5x the amount of installed memory. Remove page file from all other drives. Dedicated disk size should be larger than the page file by at least 5GBytes, suggested drive letter **P**.

ⓘ **NOTE:** Do not forget to adjust disk size and page file size if increasing server memory allocation.

3. Setup user(s) on windows servers with administrator rights for the HES installation.

4. Install a valid Server Certificate on every server designated to serve Web interface, required for Field tools to authenticate.

   Should the Organization deployment have a firm requirement for server-to-server encrypted communication, a valid Server security certificate must exist on every server of the Organization; each certificate must include the server FQDN as well as any other name designation being used for said servers in the context of a full-High Availability deployment or if generic names are being used.

(i) **NOTE:** Make sure the Certification Path is complete for every certificate on every server.

5. Ensure Windows Server is up-to-date, and subscribed to Microsoft Critical Windows updates only.

6. Time-sync through Active Directory or NTP is mandatory for every server of the Organization, including the database server.

(i) **NOTE:** Make sure all servers perform a time sync at least twice daily.

Server Policies

Enabling any of the following policies on any Windows-based servers related to ICMS, CIN or Emerge components will create problems in the Emerge installation and/ or operations.

- System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing

Linux Server Checklist

Basic Linux Network Tools

On Linux servers used to deploy Emerge components, make sure the Linux distribution being installed contains the following basic packages, required for proper product installation, operation and possible troubleshooting.

```
network-scripts (Red Hat 8.x/CentOS 8.x only)
ifupdown        (Ubutuntu 18.04 only)
tcpdump
net-tools
netstat
telnet
epel
```

(i) **NOTE:** Installation of these features may vary by Linux distribution, see related Linux installation procedures for details.

Linux Mountpoints Permissions

Java and Microsoft dotNet will require execute permissions in these `tmp` folders:

`/tmp`

`/var/tmp`

If using dedicated mountpoints for these, make sure the **noexec** option is not specified.

3
CIN Platform Preparation

Overview

CIN-UI, **ICMS** and **IAS** component prerequisites and installation steps are explained in this chapter.

Landis+Gyr recommends using a dedicated drive on all servers for application installation; this guide will use **D:** to facilitate reading.

CIN Server Preparation

Prepare the **CIN** server as follows.

Generalities

1. **ICMS** requires .**Net Framework 4.8** for proper operation. Please make sure that **CIN** server has this as the minimum version.

2. Preferred **CIN** platform is a server dedicated for this purpose and not shared with any of the Landis+Gyr product actual servers. This way, the **CIN** operator can manage many installations without having access rights to the actual servers; and the **CIN** can be used to manage multiple organizations/instances easily.

3. Provide a dedicated drive of minimum 20G, recommended 50+G (referred as **D:** drive in this document).

4. Install **Chrome** browser on **CIN** server.

ⓘ **NOTE:** Although Internet Explorer is available on most servers, Landis+Gyr strongly recommends using **Chrome** browser for **CIN-UI** operation, as it is not tested using Internet Explorer.

☀ **CAUTION: CIN-UI 6.1.0.0 and later no longer require Java OpenJDK. If upgrading the CIN-UI from a previous version, proceed as follows before continuing:**

1. Uninstall CINUI (5.x and older) using instructions provided in the Command Center Installation Using the Centralized Installer and ICMS Framework, publication number 98-2230, delivered with earlier product installation.

2. OpenJDK can be uninstalled from CIN server, and JAVA_HOME global environment variable removed.

SQL Database Preparation for ICMS

ICMS version 5.x and later is now based on a SQL Server database instead of XML database, for more scalability and robustness. Landis+Gyr recommends installation of **Microsoft SQL Server Express (SQL Express)** version 19 or later on the ICMS server, or using

any pre-existing SQL Server already available where a dedicated instance should be created for ICMS operations to ensure better access protection.

> **(i)** **NOTE:** Refer to the "Database Preparation", section "Database Passwords" on page 19 for characters to exclude from the password for sa account.

Follow these steps for database preparation before continuing with ICMS installation.

1. Get SQL Express 2019 here: https://download.microsoft.com/download/7/c/1/7c14e92e-bdcb-4f89-b7cf-93543e7112d1/SQLEXPR_x64_ENU.exe

   Installing SQL Express will automatically create a default instance named SQLEXPRESS if all defaults are used.

2. During SQL Express installation, or while preparing dedicated SQL Instance on existing SQL Server, select **Mixed mode Authentication**.

3. Get **SQL Management Studio** (optional) here: https://aka.ms/ssmsfullsetup

4. Launch **SQL Server Configuration Manager** and perform following steps (adjust instance name as needed):

   Under **SQL Server Network Configuration >> Protocols For SQLEXPRESS**:

   a. Disable **Shared Memory** and **Named Pipes**.

   b. Enable **TCP/IP**.

   c. Open **TCP/IP** properties, select **IPAddresses** tab and locate **IPAll** section at the bottom of the list:

      i. Remove any value in **TCP Dynamic Ports** (leave blank).

      ii. Set **TCP Port** to desired numerical value (cannot be left blank). The specified port must be unique to this SQL instance and not shared.

   d. Enabled changes by restarting **SQLEXPRESS** instance from **SQL Server Services >> SQL Server (SQLEXPRESS)**.

Encrypted Communications

Both **CIN-UI** and **ICMS** components support encrypted HTTPS communications. Before selecting this option during product installation, it is necessary to create a valid "server" certificate for the **CIN** server.

Import the certificate in the **Personal** store of the **Local Computer** account in **Certificate Manager**, and place the certificate's PFX file on the server, as PFX file is required for product installation. Also make sure the certification chain is valid by adding the corresponding **Root CA** and any **Intermediate CAs** in their respective certificate store in **Certificate Manager**.

> **CAUTION: Our product will auto-detect the server certificate from the Personal store. In order for this procedure to work, The CIN server certificate must comply with the following:**
>
> **1. FQDN of the CIN server must be used as the CN of the Subject of the certificate**
>
> **2. FQDN of the CIN server must be present in the SAN list of the certificate**

ⓘ   **NOTE:** Setting **ICMS** for **HTTPS** operation will also require that every server of any Organization managed by this **ICMS** are configured with **HTTPS** as well.

Installation and Configuration Management Service (ICMS)

Open an RDP session to the **CIN** server and perform the following:

⇨   *IMPORTANT: When using CIN-UI 6.1.x and later, ICMS 5.4.x or later must be used.*

Installation

⇨   *IMPORTANT:* Use HTTPS for Emerge in Google Cloud.

1. Create `D:\LandisGyr\ICMS` folder.
2. If encryption between **ICMS** and **IAS** is required, refer to "Encrypted Communications" on page 25 for details about certificate PFX preparation.

☀   **CAUTION: Many packages distributed with Emerge 2.0 and later uses features that are not supported by ICMS version 5.1.x.x and older.**

         Make sure to use the proper version of ICMS and CIN UI.

3. From an elevated DOS prompt, navigate to folder where the **ICMS** installation file `ICMSWixInstaller_X.0.0.Y.msi` is located and execute it to start **ICMS** installation. It is not possible to install the **ICMS** by right-clicking on the **.msi** file as the "Run as Administrator" option is not available for files of type **.msi**

    ICMS 5.x and later will prompt for SQL Server database information. Provide all information as follows:

Figure 3 - 1. Server Information

    a. Use `D:\LandisGyr\ICMS` as the target installation folder.

    b. **ICMS SQL Server**: (With / Without Instance Name as per SQL database preparation). For example:

        Server.FQDN\SQLEXPRESS where **Server.FQDN** is the server FQDN and **SQLEXPRESS** is the Instance Name. Note that **SQL Express** will install a named instance by default, named **SQLEXPRESS**.

        ...or...

        Server.FQDN to use the default SQL database without any instance defined, simply use

> ⓘ **NOTE:** Do NOT use `localhost` as the SQL Server hostname, even if SQL Server is installed on the same server as ICMS.

    c. **ICMS SQL System Port**: Port number of the database / instance, as configured in database preparation step in the TCP/IP properties.

    d. **ICMS SQL System User**: Administrator user account used to create the database or instance. **Default value**: `sa`

    e. **ICMS SQL System Password**: Password of system user account.

> ⓘ **NOTE:** Do not accept default, provide your own password.

    f. **ICMS Database Password**: Password for the **ICMSUser username.**

        • For first ICMS installation using SQL database, ICMSUser will be created and associated this provided password.

        • For upgrades, make sure input password matches the password defined in the database for ICMSUser.

> ⓘ **NOTE:** Refer to the "Database Preparation", section "Database Passwords" on page 19 for characters to exclude from the password for sa account.

> ⓘ **NOTE:** Do not accept default, provide your own password.

Figure 3 - 2. Server Information

More Specifically:

g. ICMS Files Dir folder will be set to `D:\ICMSFiles`

➡   *IMPORTANT: When upgrading ICMS, this value MUST be the same as previous ICMS installation to trigger the import script that will move all previous ICMS information to the SQL database.*

h. Keep **IAS** and **ICMS** ports to default values; if customizing, take note of updated values.

i. Set **CINUI Port** and **CINUI Http Protocol** values to be consistent with **CIN-UI** product installation, as per section "Centralized Installer User Interface (CIN UI)" on page 29.

j. If using **HTTPS** for **ICMS** communication, bind **ICMS** to server certificate PFX file as identified in section "Encrypted Communications" on page 25.

4. If using Windows Firewall, add an **Inbound** rule to allow **ICMS** port.

Upgrade

To upgrade the **ICMS**, follow **Step 3** of the **Installation** procedure above to perform an in-place upgrade without the need to remove existing version.

ⓘ   **NOTE:** If the in-place upgrade fails, remove previous version using instructions from **Uninstallation** section below, and install new one using **Step 3** of the **Installation** procedure above.

Uninstallation

To uninstall the **ICMS**, navigate to the 'Programs and Features' option under **Control Panel** and uninstall the **'Landis+Gyr ICMS Server'** component from the list.

ⓘ   **NOTE:** Uninstalling the ICMS service will **not** remove any database content

Centralized Installer User Interface (CIN UI)

Open an RDP session to the CIN server and perform the following:

Installation

➡️ **IMPORTANT:** Use HTTPS for Emerge in Google Cloud.

1. Create `D:\LandisGyr\CIN` folder.

2. From an elevated DOS prompt, navigate to folder where **CIN-UI** installation file `CINUIWixInstaller_6.X.0.Y.msi` is located and execute it to start **CIN-UI** installation.

   It is not possible to install the **CIN-UI** by right-clicking on the **.msi** file, as the "Run as Administrator" option is not available for files of type **.msi CIN-UI** 6.1.x and later, will prompt for various settings. Provide all information as follows:
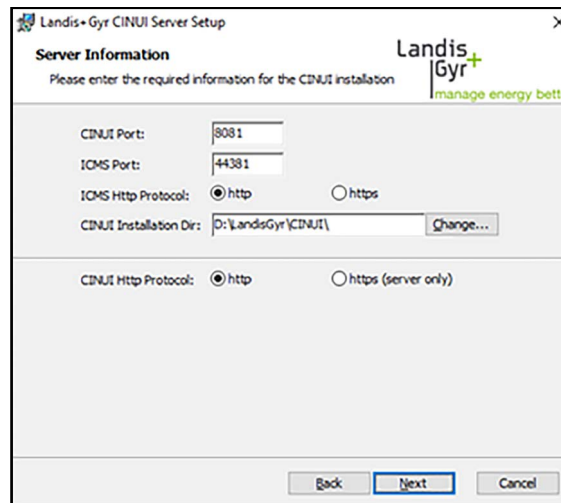
Figure 3 - 3. Server Information

   a. Set desired `CINUI Port` for UI access.

   b. Set `ICMS Port` and `ICMS Http Protocol` to be consistent with same settings selected during **ICMS** product installation, as per section "Installation and Configuration Management Service (ICMS)" on page 26".

   c. Use `D:\LandisGyr\CINUI` as the target CIN-UI installation folder.

   d. Set `CINUI Http Protocol` as required for clients to connect to **CIN-UI**.

      Refer to section "Encrypted Communications" on page 25 for **CIN** server certificate details.

3. If using Windows Firewall, add an **Inbound** rule to allow `CINUI Port`.

4. Connect to the CIN-UI http(s)://CIN.Server.FQDN:CINPort using Chrome, where:

   • http/https is the value selected for `CINUI Http Protocol`

   • CIN.Server.FQDN is the FQDN of the CIN server

   • CINPort is the value selected for `CINUI Port`

⇨ **NOTE:** The **username** input in **CIN UI** is for activity auditing only; it does not serve any security purpose as there is no validation of any form performed on **username** by **CIN UI**.

⇨ *IMPORTANT: For security reasons, Landis+Gyr does not recommend making the **CIN-UI** available remotely. It should only be made available when the operator is connected to **CIN** server using a valid RDP session to allow better access policing.*

⇨ *IMPORTANT: CIN-UI version 6.1.x introduces a brand-new presentation of information, but for all intents and purposes all the workflows remain identical to the earlier versions of **CIN-UI**.*

Upgrade

To upgrade the **CIN-UI** from version 6.1.x and later, follow **Step 3** of the "Installation" on page 26 to perform an in-place upgrade without the need to remove the existing version.

ⓘ **NOTE:** If the in-place upgrade fails, remove the previous version using instructions from "Uninstallation" on page 30, and install a new one using the "Installation" on page 26.

ⓘ **NOTE:** The <Ctrl+F5> key sequence may be required in Chrome to refresh the **CIN UI** version displayed at the bottom of the web page, as browser will cache this value from older version.

Uninstallation

To uninstall the **CINUI**, navigate to the 'Programs and Features' option under **Control Panel** and uninstall the **'Landis+Gyr CINUI Server'** component from the list.

ⓘ **NOTE:** this procedure does not apply if previous **CIN-UI** version is version 5.x and older.

Organization Preparation

The very first step is to create an organization for each (or the first) environment that will be managed from this **CIN** server. This will facilitate all the workflow procedures and allow server registration to be automated in the next step. All activities in this section are executed from the **CIN-UI** session unless indicated otherwise.

1. Click the **All Organizations** green button and select the gear icon to manage organizations. Then click the **+Add Org** button to get started on a new organization.

Figure 3 - 4. Add Org

2. Enter all information related to the desired installation.

Figure 3 - 5. Org Information

a. Organization **Name** can have spaces but **Instance Name** should not. Both can be the same if desired, but they are unique to that organization and cannot be reused in a new Organization registration in this **ICMS**.

NOTE: The **Instance Name** for an organization cannot have any special characters except '-' (hyphen) or '_' (underscore).

b. **Database Type** is PostgreSQL for Emerge; select the main database technology for this environment, some components have different requirements they will be treated differently later.

c. **Confidentiality Settings Policy** can allow to store credentials provided later in organization settings as encrypted and saved (**Encrypt And Save** menu item), or not saving (**Do Not Save, Always Prompt** menu item) in which case prompts will pop-up as needed.

When selecting **Encrypt and Save** option, a menu will pop-up to provide password that will allow the encryption.

NOTE: This password is applied at the organization level; any user registered in this ICMS that has the password will be able to perform configuration and installation steps for this Organization.

NOTE: Once prompted for Organization password, **ICMS** will keep the password in memory up to 60 minutes of inactivity; make sure to avoid leaving Chrome active on the **Active** Dashboard with auto-refresh enabled as this will prevent **ICMS** from timing out on password retention.

d. Click **Save** to save organization information then **Close** the organization list.

3. Click the **All Organization** green button and select the newly created organization to load it in the current **CIN-UI** session so that all further operations are tied to this organization.
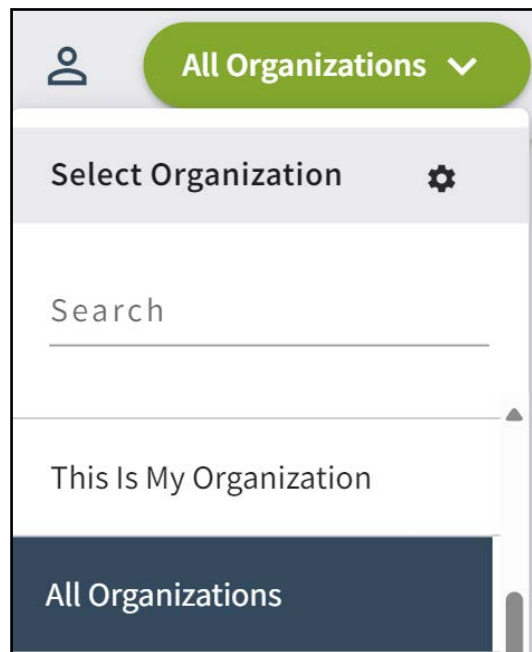
Figure 3 - 6. All Organizations

Server Preparation

Landis+Gyr Components

The **IAS** component must be installed on every server where a Landis+Gyr **ICMS**-compatible product will be deployed.

IAS versions running on Windows servers requires .**Net Framework 4.8** or later for proper operation. **IASLinux** running on Linux servers requires ASPNet Core 2.1 for proper operation.

CAUTION: IAS component will perform software installation and manipulate system settings on the server where it runs. This is required to allow proper Landis+Gyr software operation. As such, each IAS component is required to run with a privileged account (IASWindows will run using Local System account, while IASLinux will run using root account).

If this constitutes a breach in your internal security policies, please proceed as follows:

1. Stop and disable IASWindows and IASLinux services on all remote servers when no remote activities need to be performed using Centralized installer; and

2. Enable and start IASWindows and IASLinux services on select / all remote servers before performing remote activities using Centralized Installer.

IAS Windows

Installation

➡ IMPORTANT: Use HTTPS for Emerge in Google Cloud.

ⓘ **NOTE:** Initial installation of the I**nstallation Agent Service (IAS)** on all Windows servers must be performed manually.

Repeat the following steps on each Windows server.

1. Create folder `D:\LandisGyr\IAS`

2. If encryption between **ICMS** and **IAS** is required, prepare a "server" certificate in **.PFX** format with passphrase protection. Place it on the server.

3. From an elevated DOS prompt, navigate to folder where the **IAS** installation file `IASWixInstaller_X.0.0.Y.msi` is located and execute it to start **IAS** installation.

Figure 3 - 7. IAS Installation Location

More Specifically:

a. Use `D:\LandisGyr\IAS` as the target installation folder.

b. Use **IAS** and **ICMS** ports as specified during **ICMS** product installation.

c. **ICMS Server** value should be set to the FQDN of the **CIN** server

d. **Org Instance Name** value should be set to the actual **Instance Name** defined in the organization preparation.

ⓘ   **NOTE:** Org Instance Name value is case sensitive.

e. **IAS Files Dir** value should be set to `D:\IASFiles`

f. Make sure option **Register with ICMS** is selected.

g. If using **HTTPS** for **ICMS** communication, bind **IAS** to server certificate.

4. If using Windows Firewall, add an **Inbound** rule to allow **IAS** port from **CIN** server.

Upgrade

Upgrade of the **Installation Agent Service (IAS)** can be performed two ways:

1. *Using ICMS*: IAS for Windows version can be easily upgraded remotely using the ICMS. Follow the procedures in this guide to import the new **IASWindows** component, and

a. If it is the first **IASWindows** upgrade, create a profile containing target **IASWindows** component, and simply deploy it to all Windows servers of the Organization using the standard ICMS installation procedure. No settings are needed, everything currently used on the target server will be re-used during the upgrade process, including HTTPS certificate binding.

b. If there is already an **IASWindows** profile deployed to servers, use Smart Upgrade or the regular upgrade procedure documented below to upgrade **IASWindows** on all Windows servers of the Organization.

☀   **CAUTION: ICMS upgrade of IAS Windows component is not possible when server was build using a language different than US English. If it's the case, manual upgrade of IAS Windows is required.**

2. *Manual Upgrade*: It is possible to perform an in-place upgrade by manually running the WIX Installer (`IASWixInstaller_X.0.0.Y.msi`) of the new **IAS for Windows** version from an elevated DOS prompt on all Windows servers, following the **IAS Windows - Installation - Step 3** procedure documented above.

ⓘ   **NOTE:** If the in-place upgrade fails, remove previous version using instructions from **Uninstallation** section below, and install new one using **Step 3** of the **Installation** procedure above.

Uninstallation

Uninstalling the **Installation Agent Service (IAS)** can be performed as follows:

1. If **IASWindows** was upgraded through ICMS, perform the "**Remove**" operation using CIN UI to remove the **IASWindows** profile deployed on the Windows server(s) where the IAS should be removed.

2. In all uninstallation cases, connect to the Windows server using RDP session, navigate to the 'Programs and Features' option under Control Panel and uninstall the '**Landis+Gyr Installation Agent Service**' component from the list.

IASLinux

Repeat the following steps on each Linux server.

Preparation

1. If encryption between **ICMS** and **IASLinux** is required, prepare a "server" certificate in .**PFX** format with password protection. Place it on the server.

(i) **NOTE:** PFX password cannot contain any `space` character nor any of the following:

> `' " ` $ \ & ;`

Installation

⇨ *IMPORTANT:* Use HTTPS for Emerge in Google Cloud.

1. Edit the IAS installation script `installIAS-0.0.0.0.sh` and modify the following values:
   - **ICMS_SERVER**: Value should be set to the FQDN of the CIN server.
   - **HTTP_PROTOCOL**: Set the value to HTTPS to establish communication with ICMS.
   - **REGISTER_WITH_ICMS_SERVER**: Value should be set to TRUE to enable auto-registration with ICMS, or set to FALSE otherwise.
   - I**AS_REST_PORT, ICMS_REST_PORT**: Should be set to the values used during ICMS product installation.
   - **ORG_INSTANCE_NAME**: Value should be set to the actual Instance Name defined in the organization preparation.
2. If using **HTTPS** for **ICMS** communication, then modify the following values in the same script:
   - **HTTPS_ROOT_CA**: full path and file name of the Root CA certificate.
   - **HTTPS_CERT_PFX_FILE**: Value should be set to the path where local server certificate (in .**PFX** format) is stored.
   - **HTTPS_CERT_PFX_FILE_PASSWORD**: Value should be set to the password of the local server certificate.
3. Install IASLinux using the command:

```
sudo ./installIAS-0.0.0.0.sh
```

(i) **NOTE:** Depending on how the **IASLinux** package was copied to the Linux server, it may be required to change the execution mode of the install script to allow execution.

4. From the **CIN-UI** session, select the **Servers** button from the side ribbon and observe the FQDN of this server is now showing in the list of servers available to this organization.

(i)   **NOTE:** For new Linux servers that have never registered with ICMS, if **REGISTER_WITH_ICMS_SERVER** value is set to **false** in the installation script, the server will not show in the **Servers** list in **CIN UI**.

Upgrade

The Installation Agent Service (IAS) can be upgraded in two ways:

1. *Using ICMS*: IAS for Linux can be easily upgraded remotely using the ICMS. Follow the procedures in this guide to import the new **IASLinux** component, and

   a. If it is the first **IASLinux** upgrade, create a profile containing target IASLinux component, and simply deploy it to all Linux servers of the Organization using the standard ICMS installation procedure. No settings are needed, everything currently used on the target server will be re-used during the upgrade process, including HTTPS certificate information.

   b. If there is already an **IASLinux** profile deployed to servers, use Smart Upgrade or the regular upgrade procedure documented below to upgrade **IASLinux** on all Linux servers of the Organization.

2. *Manual Upgrade*: To manually upgrade the **IASLinux**, copy all settings from the currently installed version of the **IASLinux** to the new version install script and install the newer version. Older **IASLinux** will be uninstalled when running the new install script.

Uninstallation

To uninstall the **IASLinux**, navigate to the folder where the **IASLinux** installation files (compatible with the Linux version being used) are located and run the following command:

```
sudo ./<uninstallAS.sh>
```

(i)   **NOTE:** Depending on how the **IASLinux** package was copied to the Linux server, it may be required to change the execution mode of the uninstall script to allow execution.

Registered Servers

From the **CIN-UI** session, select the S**ervers** button from the side ribbon and observe the FQDN of this server is now showing in the list of servers available to this organization.
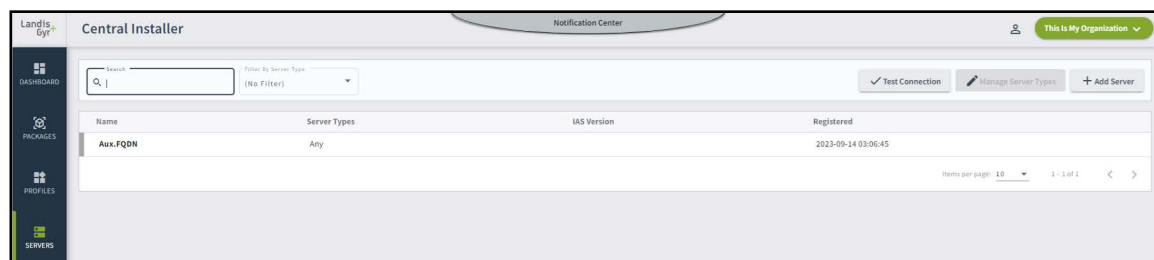
Figure 3 - 8. Server Registered in Organization

ⓘ   **NOTE:** On this list, the **Server Type** value can be set to allow **Smart Install** feature to match profiles to server types during installation.

Third-Party Components

LunaSA Client

If the Organization will use Landis+Gyr Advanced Security option, every server where **CCApp** and **KeyManagerApp** components are installed will require the **SafeNet/Gemalto LunaSA Client**, as provided by Landis+Gyr. The version of the client will have to match the version of the **SafeNet/Gemalto Hardware Security Module (HSM) Appliances**, consult Landis+Gyr for proper version.

The **LunaSA** client is available as an ICMS-based installation as well as stand-alone MSI-based installation. Landis+Gyr recommends installation of the Luna client be performed as per document, *ICMS Installation Add-On: ANSI Adapter Package Specifics*, 98-2570.

⇨   *IMPORTANT: Luna client manual installation should not be performed unless recommended by Landis+Gyr.*

Others

Any customer-specific third-party components can be installed at this point.

4
Preparation Workflow

Overview

Now that servers are registered in the current organization, configuration work may start.

Import ICMS Packages

The following steps are required for a new installation or every upgrade based on ICMS.

1. Obtain latest version of the **WindowsPrerequisites** ICMS package, as a ZIP file. Place it on **CIN** server in `D:\ICMSFiles\ImportPackage` folder. Do not unzip.

ⓘ **NOTE:** Landis+Gyr may provide additional prerequisites packages for some additional components; they should all be imported in CIN using same procedure.

2. Obtain all Landis+Gyr product ICMS packages relevant for installation, as a collection of ZIP files. Place them on **CIN** server in `D:\ICMSFiles\ImportPackage` folder. Do not unzip.

3. From **CIN-UI** click the **Packages** button from the side ribbon, then click the **+Import packages** button.
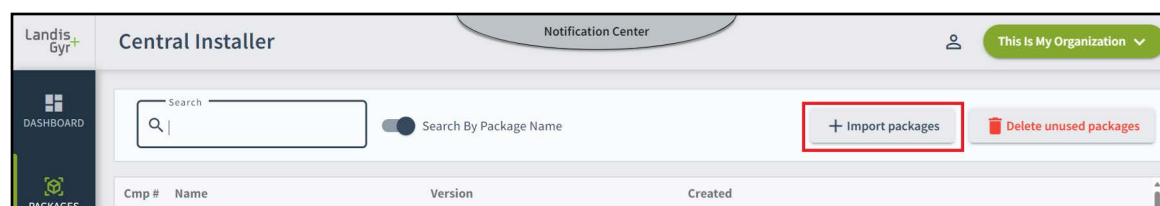
Figure 4 - 1. Import Packages

4. The list presented will be representative of all the ZIP files located in `D:\ICMSFiles\ImportPackages`. From the list, select all packages and follow the workflow to complete the import.

5. Repeat steps 1 to 4 for **Linux Prerequisites** ICMS package, if Organization contains Linux-based components (Kafka, Tunnel Manager, IP Gateway, etc...)

⇨ *IMPORTANT: Linux distributions vary widely by version and selected options at installation time. While we do our best to ascertain our prerequisites will include the base version of known Linux dependencies, there could be cases where some Linux prerequisites may fail installation because of a missing dependency in the base image provided for product installation. This is out of Landis+Gyr control. If this situation happens, the error message for the failed component in CIN UI will identify the missing dependency; please proceed to manual installation of missing dependency and retry Landis+Gyr component installation. We apologize for the inconvenience.*

CAUTION: Emerge 2.1 introduces an enhanced method for patching. Each ICMS package now contains scripts to stop and start all components that can be deployed by this package. These scripts will be used primarily for patching.

The exact name of these stop/start components will vary by package and thus are not listed explicitly in any ICMS Add-On documents.

Building Server Profiles

With ICMS framework, server functionality is grouped in a logical way under a **Profile**. For instance, if a server consolidates Emerge Web and Application, a corresponding profile could be created and named "Emerge_Web-App". Should many servers be part of a same configuration under high availability configuration, they will all be assigned to the same profile, and ICMS will automatically change any custom values for each server.

All ICMS packages have built-in dependencies, possibly linking them to other ICMS packages and/or to prerequisites required for proper operation. As a rule and to simplify profile management, Profiles are created based on actual Landis+Gyr product components and ICMS will automatically add the related prerequisites as dependencies. This way the operator does not need to know which part of the prerequisites need to be assigned to support specific ICMS packages, this is all built-in as dependencies in each ICMS component. Similarly, during the installation workflow, there are additional dependencies between ICMS packages and components to make sure that should one specific component requires another one, it will not be installed if the missing component is not existing already. A good example of this would be that if an application component requires a corresponding DB component for operation, one would not be able to deploy said application profile until the corresponding DB profile is actually reported as being "Installed" by the ICMS.

Consult **ICMS Installation AddOn** document of every package part of each Organization for any profile-specific information of each package.

Profile Naming Convention

Profile naming convention is important. Make sure the profile name is meaningful to the **CIN** operator to ease deployment and maintenance. In the profile name, include an underscore character immediately followed by the build number of the package holding the Landis+Gyr components part of the profile. For instance all components of the same Emerge package will bear the same version number.

Profiles - New Install

To complete **ICMS** preparation, initial **Profiles** must be created. Make sure to group ICMS components in logical profiles that will adequately represent the role of each server of the Organization.

Profiles and Packages

Although not mandatory, it is highly recommended to avoid mixing components from different packages in the same profile. Building profiles with only components from same package will greatly facilitate installation workflow and later patching if required. But it should be noted that a profile cannot be applied to a server if the DB component and the corresponding application component are part of the same said profile. Hence, it is required for a DB component to be included in a separate profile than the corresponding application

component. In general, a database profile would be applied only once per organization installation whereas application profiles can be applied on a larger number of servers.

ⓘ **NOTE:** It is possible to assign many profiles to the same server, in cases where components from various packages need to coexist on same server.

DB Profile Particulars

All application components have a dependency on the corresponding DB component being part of a **separate** profile that requires to be applied in **ICMS** before the said application is installed.

Database profiles will NOT be applied from the database server itself, the **ICMS** will use any server registered to the Organization to run a series of scripts that will remotely apply proper configuration and settings to the corresponding database.

Creating New Profiles

1. To add **Profiles** in ICMS, click the **Profiles** button on the side ribbon, then select **+Add profile**.
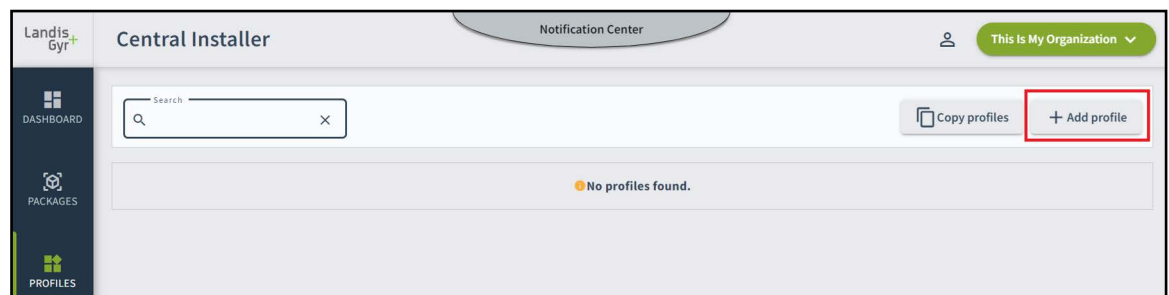
Figure 4 - 2. Add Profile

2. Enter desired **Profile** name and click **+Save**. Landis+Gyr recommends respecting the naming convention for profile names.

Figure 4 - 3. Add Profile Name

3. From the profiles list, click on the newly created **Profile Name** and select **+Add Components**.
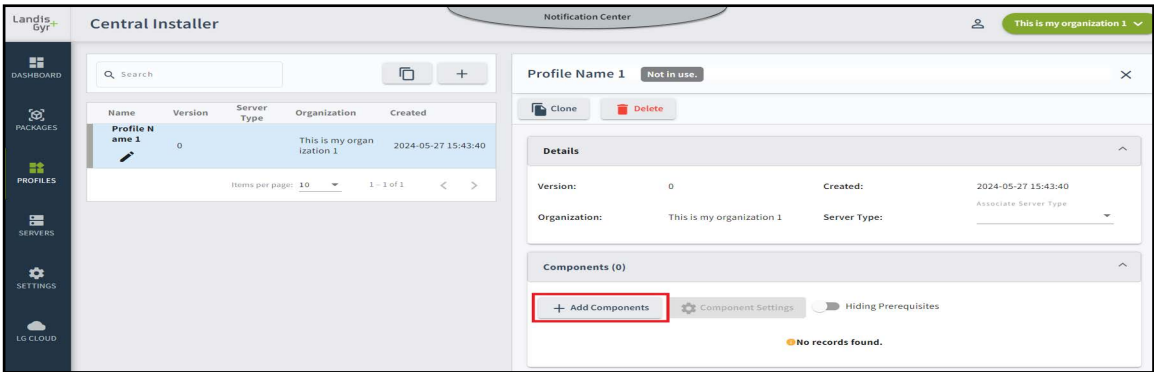
Figure 4 - 4. Add Components

4. Select desired Landis+Gyr product components that will be part of this server profile and click **Next** to review the selection, then **Confirm** selection to save the profile.

(i) NOTE: Selecting the Pencil icon next to a profile name allows renaming a profile that was not assigned to any server, while clicking anywhere else on the profile line will allow adding components to an unassigned profile.

Do not select any components related to any prerequisite package, they will be automatically added to the profile based on product component selection.

When selecting product components, please verify the version information with the Release Notes of the Emerge version being configured for this Organization, to avoid any version mismatch.

Once a profile is assigned to a server, its components selection cannot be changed.

Table 4 - 1, "Profiles to Server Associations," suggests application profiles to server associations components based on various deployments. This list is not authoritative nor does it include all possible combinations. Database profiles are not considered here. Build references are omitted to shorten names.

(i) NOTE: Table 4 - 1 does not include additional components related to RF Mesh Deployments with Platform-Based Endpoints

---

(i) NOTE: Profiles to server associations must conform to information set forth in each **ICMS Installation AddOn** document of every package part of the Organization. Table 4 - 1, "Profiles to Server Associations," is for illustrative purpose only.

Table 4 - 1. Profiles to Server Associations

Server Tier	Profiles Associated to Each Server in Tier
Organization style RF Mesh only without Advanced Security, single-server Organization, no Integration	
Emerge	Emerge-Single
Organization style RF Mesh with PLX, Advanced Security, small multi-server Organization, with Integration Suite with DA/ SCADA	
Emerge Web	EmergeWeb-PLX
Emerge Application	EmergeApp-AS

Table 4 - 1. Profiles to Server Associations (Continued)

Server Tier	Profiles Associated to Each Server in Tier
Integration Suite	IS
Organization style RF Mesh IP with Advanced Security, entry-level Organization, with Integration Suite, no DA/SCADA	
Emerge	Emerge-Single-GND, ANSI, DeviceHub
Integration Suite	IS
RF Mesh IP	MeshIP
Organization style RF Mesh with Advanced Security, split Integration Suite, multi-server HA configuration	
Emerge Web + IS API	EmergeWeb, IS-API
Emerge Primary App	EmergePri-AS
Emerge Aux + IS Mess. Handlers	EmergeAux-AS, IS-MH
Organization style RF Mesh IP (with/without RF Mesh) with Advanced Security, Integration Suite, multi-server HA configuration	
Emerge Web	EmergeWeb
Emerge Primary App	EmergePri-AS
Emerge Auxiliary App	EmergeAux-AS-GND, ANSI, DeviceHub
Integration Suite	IS
RF Mesh IP	RFMeshIP
Organization style RF Mesh IP and M2M with Advanced Security, split Integration Suite, multi-server HA configuration	
Emerge Web + IS API	EmergeWeb, IS-API
Emerge Primary App	EmergePri-AS
Emerge Auxiliary App	EmergeAux-AS-GND, ANSI, DeviceHub, IS-MH
RF Mesh IP	RFMeshIP
M2M Cellular	M2M

Once all profiles of a new Organization are created and required profile overrides completed, proceed to the **Installation Workflow** section.

Profile Overrides

In cases where values for any component need to be refined beyond what is exposed in the **Settings** page of the **CIN-UI**, profile-level overrides can be used. In some cases, profile overrides are actually required for proper installation.

ⓘ   **NOTE:** Any profile override will be carried forward during an upgrade operation as long as profiles are cloned *or* **Smart Upgrade** is being used. Details on upgrade strategies are discussed later.

Consult **ICMS Installation Add-On** document of every package part of each Organization for any package-specific Profile Overrides settings that need to be configured.

Profile Override - General Procedure

Should any profile of the Organization require profile-level overrides, perform these adjustments here. From the **Profiles** button of the side ribbon, click the profile that requires overrides and select **Component Settings** button.

Figure 4 - 5. Component Settings

From the list, select the component that contains the setting to override, change value(s), and save changes. Repeat as needed.

Profiles - Upgrading

If the Organization is already deployed with **ICMS** and upgrading to a newer version of Emerge, follow this procedure.

ICMS Packages

Obtain every ICMS package (.ZIP files) related to the new Emerge version and place them on the **D:\ICMSFiles\ImportPackages** folder of **CIN** server. Make sure to obtain the latest version of **Prerequisites** packages.

In **CIN-UI**, import new ICMS packages and updated **Prerequisites** packages.

Review Settings

In **CIN-UI**, select **Settings** button of the side ribbon, and review all settings of all tabs, since any new package could expose new settings for Organization configuration.

Option 1 - Clone Profiles

Once all settings are reviewed, upgrade each profile to a new version. Select Profiles button from side ribbon, then for each profile, perform the following:

1. Select the profile.Click the **Clone** button, rename the new profile to reflect new product version, then click **Next**.

Figure 4 - 6. Clone Profile

2. From the list, select only new versions of Landis+Gyr products to replace existing versions of the old profile. Each Landis+Gyr component listed will have a selection mark next to it to the right while additional components inherited in the profile by dependencies are not marked; those marked items are the components that need to be updated to keep new profile consistent with existing one.

    Tip - *Use search box by simply typing a character sequence to narrow down the list.*

3. Click **Next** to display the final list of selected components part of the profile, and make sure that for all Landis+Gyr product components the indicated version is consistent with the product version that will be installed on this Organization. Click **Back** to adjust, or **Clone** to proceed.

NOTE: Should any profile component association changes be required, it can be done during this phase. Be careful that for each change the Organization is not compromised by omitting one mandatory component that might have been removed from a profile but not added to another one.

Option 2 - Smart Upgrade

The **Smart Upgrade** is an option that allows direct upgrading from one Emerge version to the next of the same branch, with no further interactions. It does not allow to change profile content nor server assignment. If using **Smart Upgrade** option, proceed directly to **Upgrading Existing Organization**.

(i) | **NOTE:** Smart Upgrade only applies to minor versions of the same major version (7.3GA to 7.3MR1, 7.3MR1 to 7.3MR3, etc…). It would not allow upgrading from 7.3 to 7.4 major version.

Profiles - Patching

If the Organization is already deployed with **ICMS** and requires to be patched, follow this procedure.

ICMS Packages

Obtain the ICMS package (.ZIP file) related to the patch and place them in the **D:\ICMSFiles\ImportPackages** folder of CIN server.

Ensure that all the dependencies for the ICMS patch package have been imported on the CINUI (which typically includes all previous ICMS patch packages associated with the current Emerge version.)

Option 1 - Clone Profiles

Once all settings are reviewed, upgrade each profile to a new version with the patch components. Select Profiles

button from side ribbon, then for each profile that has components that need to be patched, perform the following:

1. Select the profile.Click the **Clone** button, rename the new profile to reflect new patch version, then click **Next**.
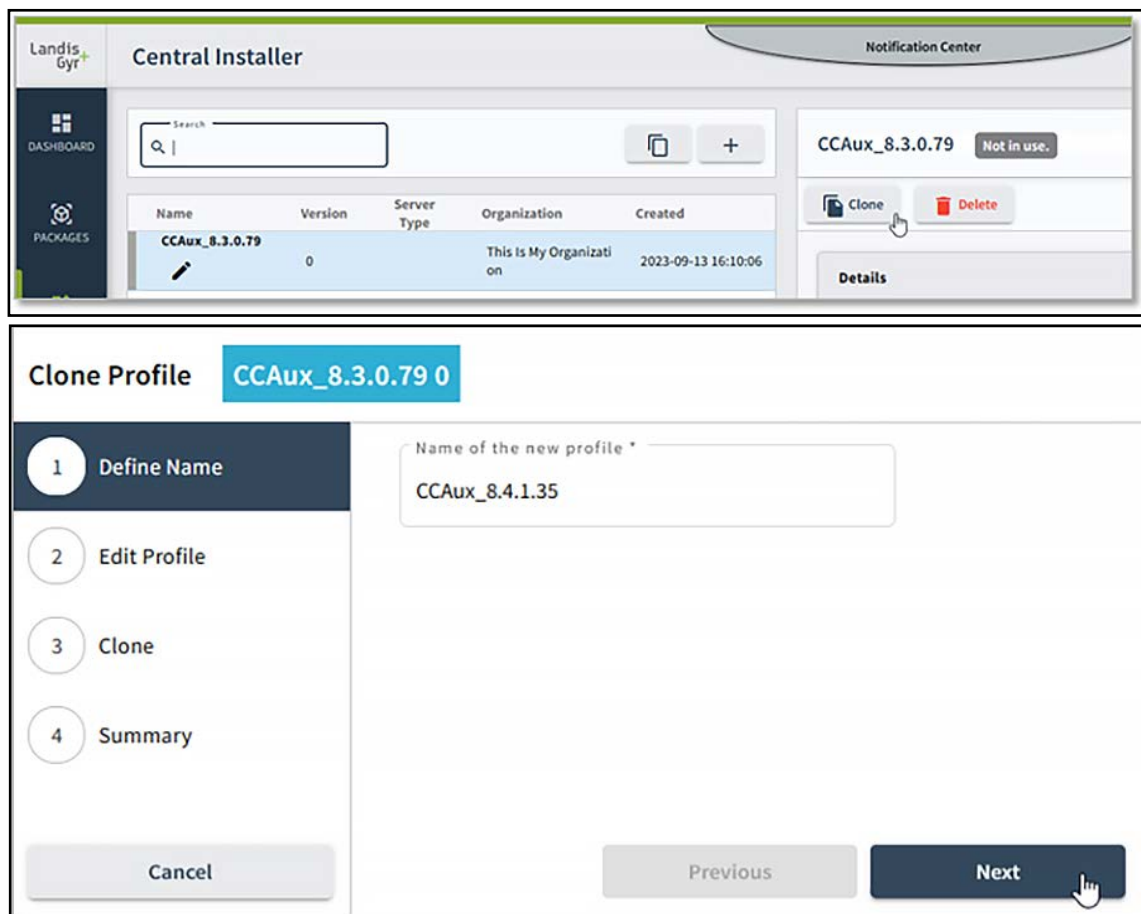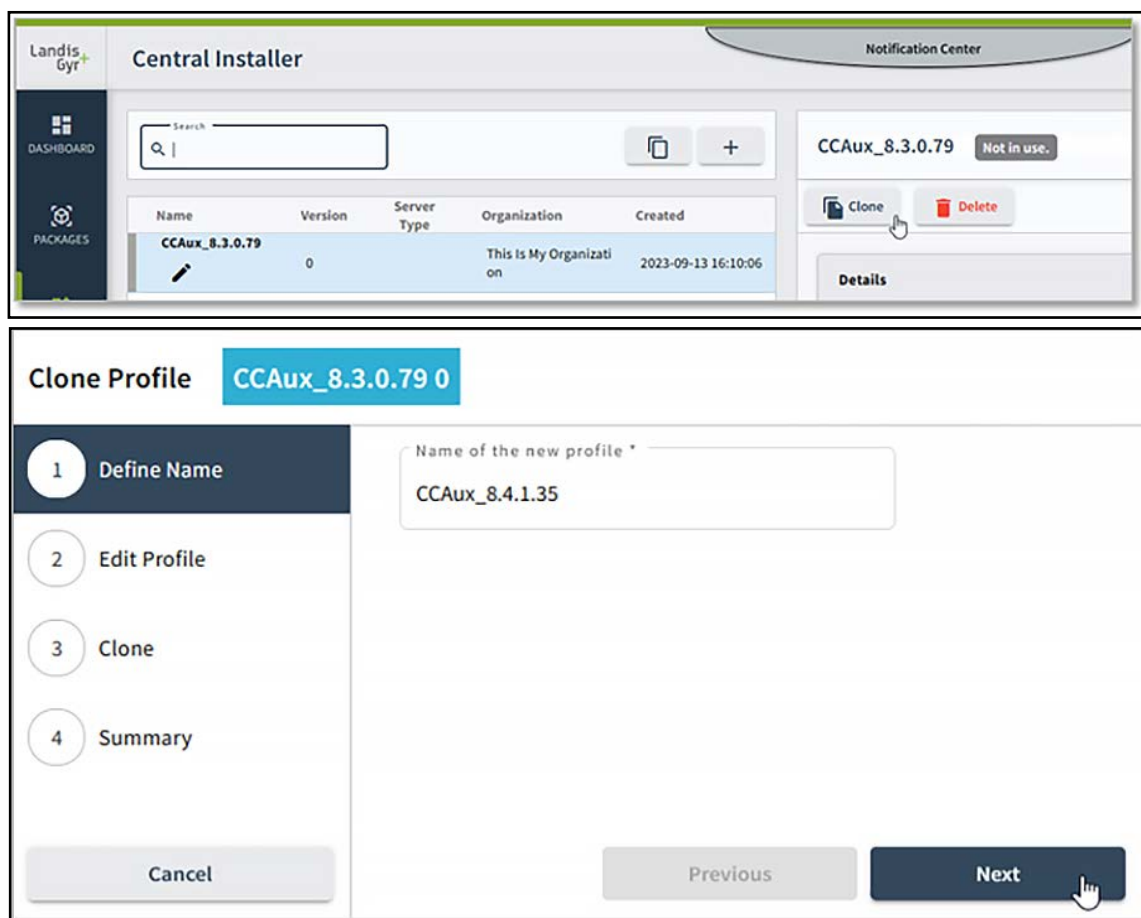
Figure 4 - 7. Clone Profile

2. From the list, select only the patch components applicable to the profile.

3. Click **Next** to display the final list of selected components part of the profile, and make sure that for all Landis+Gyr product components the indicated version is consistent with the product version that will be installed on this Organization. Click **Back** to adjust, or **Clone** to proceed.

Option 2 - Smart Upgrade

The **Smart Upgrade** also allows direct patching of deployed Emerge builds, with no further interactions. It does not allow to change profile content nor server assignment. If using **Smart Upgrade** option, refer to Chapter 5 Section 4.2.3 **Smart Upgrade**, for steps involved.

Server Overrides

In some cases you will need to apply an override at the server-level instead of profile-level. This is done as part of the actual installation workflow. See "Server-Level Overrides" on page 61 for more information.

Set and Review All Settings

Now that all necessary packages are imported in the **ICMS** and the profiles required for the organization have been created, configuration can be adjusted for this organization

deployment. From the **CIN-UI** select the **Settings** button from the side ribbon to adjust all settings. This page is organized by grouping options in various tabs. Some tabs are for general settings that will apply across all the organization components, some tabs present application-specific options applicable to specific modules including their respective database-specific information. Proceed to fill all settings of the Organization with proper values. Some values are mandatory on some tabs (e.g. all passwords); the **Save** button will not become active until all mandatory values have been assigned a value.Figure 4 - 8 presents a typical view of the **Settings** structure for an Organization but actual tabs will vary.
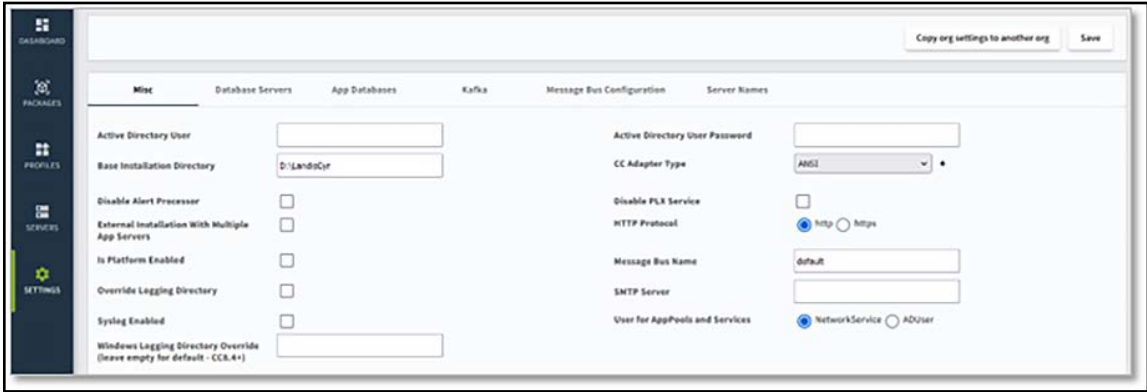
Figure 4 - 8. Settings

(i)   **NOTE:** Tabs list and content are driven by the components that have been added to the profiles specific to the current organization. If the same **ICMS** is being used to maintain organizations with different product requirements, then the Settings page will only display tabs for the components that have been included in profiles specific to the current organization.

General Settings Tabs

Misc.

This tab presents configuration settings that apply across all the Organization. It will contain all mandatory values for every Organization deployment as well as optional values dictated by some packages. Table below presents all mandatory settings based on core Emerge packages.

Table 4 - 2. Misc Tab

Setting	Description
Base Installation Directory	The base folder where all Landis+Gyr products will be nested under at installation. This will be the same across all components of any profiles of the Organization. Each component will nest its own installation folder under this one. Landis+Gyr strongly recommends using a dedicated drive for application installation; in this case because the **Base Installation Directory** is the same across all components, every server of the Organization will have to use the same drive letter for the application deployment. **Default value**: `D:\LandisGyr`

NOTE: The default logs folder location will be: `Base Installation Directory\Logs`

Table 4 - 2. Misc Tab (Continued)

Setting	Description
HTTP Protocol	Indicate if the protocol for server-to-server communication across the entire Organization must be encrypted or not. Select **HTTPS** to use transport-level encryption. Note that using **HTTPS** requires a valid security certificate to exist on every server of the Organization; each certificate must include the server FQDN as well as any other name designation being used for said servers in the context of a full-High Availability deployment or if generic names are being used. Each certificate must have a valid certification path. See **SSL Bindings** section below for additional details.
IMPORTANT: When `HTTP Protocol` is set to **HTTPS**, the installation procedure will perform an additional hardening step in IIS to disable HTTP protocol binding from the IP address of each server, only allowing HTTP traffic to be used on port 80 of the localhost IP addresses `127.0.0.1` and `[::1]`. **NOTE:** Use HTTPS for Emerge in Google Cloud. Should any Emerge component require usage of HTTP protocol, its corresponding ICMS Add-On document will indicate proper configuration details in its **Profile Overrides** section. In cases where HTTP protocol must still be used (e.g., using PLX technology), refer to **SSL Bindings** section below for details.	
External installation with multiple App Servers	Select this option if this Organization will have two Emerge application profiles where **EmergeApp** component will be assigned: • Primary • Auxiliary
Disable PLX Service	Select this option if the Organization is not using PLX-based devices. This will disable the corresponding PLX service after installation of the **EmergeApp** component.
Use Platform GND Converter	Select this option if the Organization contains **RF Mesh IP** endpoints.
User for AppPools and Services	Select which user account to use for IIS App Pools and Windows Services. Default is **NetworkService**. AD accounts are entered as **Domain\User** and will be applied to all Windows services and IIS App Pool identities in this Organization. If any component must use different identity, use a profile override.
NOTE: **User for App Pools and Services** default identity is now set to **NetworkService** and usage of **LocalSystem** is no longer supported. When upgrading an Organization, ensure to make a selection to prevent erratic installation behavior.	
IMPORTANT: Some components of various Add-Ons can be configured to generate reports on server folders. It will be necessary to manually grant "Modify" permissions for the selected **User for App Pools and Services** identity to these folders to allow processes to place the reports where configured.	
SMTP Server	Use this value to capture FQDN of the SMTP server that will be used to relay email messages to subscribers. Emerge has a built-in feature allowing its users to subscribe to certain events that can be relayed to them as email alerts. • The **Performance Monitoring Dashboards** components will use this setting to configure email alerts for critical monitoring conditions.

Table 4 - 2. Misc Tab (Continued)

Setting	Description
ODAC Base Installation Directory	The base folder where the **Oracle Data Access Client** will be nested under at installation. This is only applicable to Oracle DB-based installations and will be the same across all components of any profiles of the Organization. **ODAC Base Installation Directory** is the same across all components and hence every server of the Organization will have to use the same drive letter for **ODAC** deployment.
Is Platform Enabled	Select this option if this Organization will have any components that will be using the **Kafka Message-Bus**.
Message Bus Name	Set this value to current Organization **Instance Name** (not the name) Instance (or domain) for each topic of this Organization. When using shared Kafka messaging system across multiple Organizations, this value needs to be unique to each Organization. **Note**: This value is case sensitive and cannot contain any special characters nor spaces, only regular letters and numbers.
Emerge Adapter Type	Indicates meter protocol to use by the Adapters. Select: **ABNT** for Brazil only. **DLMS** for APAC only when DLMS meters are used. **ANSI** for all other regions.
DLMS device drivers folder	Default value: `driver` Folder containing device drivers' JAR files, under the main application installation folder
Syslog Enabled	Enables all Emerge components to send **ERROR**-level messages to identified **syslog receiver** (see **Server Names** tab). **Note**: Packages where components do not support syslog will have indication in this regard in their own Add-On document.
Syslog msg incl. hostname	Optional. When enabled, hostname value will explicitly be added to all syslog messages issued by any component. Setting only visible when **Syslog Enabled** option is selected. Most syslog receivers do not require this option as they will add the hostname automatically.
Syslog msg incl. timestamp	Optional. When enabled, timestamp will explicitly be added to all syslog messages issued by any component. Setting only visible when **Syslog Enabled** option is selected. Most syslog receivers do not require this option as they will add the timestamp automatically.
Windows Logging Directory Override	When left blank, logging base folder will be nested under the `Base Installation Directory`. If logging base folder needs to be set to a different location, enter the full path of the parent folder where `Logs` folder will be created and where all components will put their log files. **Default value**: `<blank>`

Server Names

This tab presents configuration settings pertaining to internal data flow between components of the Organization. Values proposed here are defined in **Service URL Definitions** table, consult it for details.

(i) **NOTE:** Elements presented in the **Server Names** tab will vary based on packages imported in **ICMS**.

Table 4 - 3. Server Names

Server "Server Names"	Description
Emerge Primary App Server Name	Use value **Inbound-to-EmergePri**
Emerge Application Layer	Use value **Inbound-to-EmergeApp** or set to **Inbound-to-EmergePri** if current **Organization** has a single server hosting **EmergeApp** component.
Integration Services Server Name	Use value **Inbound-to-ISMH** or set to **localhost** if not used.
RF Mesh IP Server Name	Use value **Inbound-to-MeshIP** or set to **localhost** if not used.
M2MAdapter Server Name	Use value **Inbound-to-M2M** or set to **localhost** if not used.
ABNTAdapter Server Name[1]	Use value **Inbound-to-ABNT** or set to **localhost** if not used.
CMAdapter Server Name[1]	Use value **Inbound-to-CMA** or set to **localhost** if not used.
RFAdapter Server Name[2]	Use value **Inbound-to-RFA** or set to **localhost** if not used.
DLMSAdapter Server Name[2]	Use value **Inbound-to-DLMS** or set to **localhost** if not used.
6N76Adapter Server Name[2]	Use value **Inbound-to-6N76** or set to **localhost** if not used.
PLX App Server Name	Use value **Inbound-to-EmergeApp** or set to **Inbound-to-EmergePri** if current Organization has a single server hosting **EmergeApp** component or set to **localhost** if not used.
Kafka MessageBus Server	FQDN or IP Address for Kafka broker(s). When using a Kafka cluster, this value will be comma-separated list of **FQDNkafka1,FQDNkafka2,FQDNkafka3** or **IPkafka1,IPkafka2,IPkafka3** without any white spaces. **Note**: IP addresses should not be used if `Kafka TLS` option is enabled.
Elasticsearch Server	FQDN or IP Address for Elastic search server used by some components for reporting/logging.
WiSun Adapter Server Name	Use value **Inbound-to-WiSUN** or set to **localhost** if not used.
Syslog Receiver	FQDN of syslog receiver where syslog messages will be sent, in UDP packets. Only visible when **Syslog Enabled** option is selected on the **Misc** tab. Adjust the **Syslog UDP Port** in the Service Ports frame below as needed. **Note**: Encryption is not supported in UDP syslog messages, which is the only option supported by logging libraries in use in Landis+Gyr components.

[1] Brazil-specific, not defined in Service URL Definitions table.

[2] Japan-specific, not defined in Service URL Definitions table

Server Names tab presents a **Service Ports** section presenting all service ports that can be customized. The name each customizable service port refers to the component that offers that service.

(i) **NOTE:** Landis+Gyr recommends keeping the default values for all service ports.

Database Servers Tab

This tab presents database settings that apply across all components. The content is driven by the default Organization DB type plus any overrides that may be performed in the **App Databases** tab.

Table 4 - 4. Database Servers Tab

Database Servers Setting	Description
Database Server	FQDN or IP address of the database server serving for this module of the current Organization. **SQL Server only:** if using Named Instance, use **FQDN\NamedInstance** notation.
Database Port	**If SQL Server DB** - specify the port to use to reach this SQL Server database. **If Oracle DB** - port of the TNS Listener corresponding to the DB SID. Cannot be left blank.
Oracle Database SID	**For Oracle only** - Oracle SID hosting the DB for this module. Cannot be left blank.
Tablespace Directory	**For Oracle only** - tablespace location. For Oracle installation on Solaris or any UNIX based platform, it is required to terminate the path name with a "/" (e.g. `/oradata/ThisFolder/` or `+DATA/ThisFolder/`) For Oracle installation on Window platform, it is required to terminate the path name with a "\" (e.g. `D:\oradata\ThisFolder\`)
Database System User	DB account with system-like rights, required for module installation. This account can be locked and temporarily unlocked during installation / maintenance window.
Database System Password	Password of the corresponding DB account with system-like rights.

⚠ **WARNING:** The **App Databases** tab will contain all DB-related application accounts and credentials for all components that require database utilization.
Please consult **Appendix C** for important information about password rotation for these DB Application accounts**.**

Message Bus Configuration

The **Message Bus Configuration** tab presents configuration settings that apply across all the Organization, directly related to **Kafka Messaging** system operation. When Organization requires **Kafka** for messaging between components, all values from this tab must be filled.

Table 4 - 5. Message Bus Configuration Tab

Setting	Description
Message Bus Broker Address Family	Use this setting to indicate if **IPv4** or **IPv6** protocol will be used to communicate with Kafka broker(s).

Table 4 - 5. Message Bus Configuration Tab (Continued)

Setting	Description
Message Bus Name	Set this value to current Organization **Instance Name** (not the name) Instance (or domain) for each topic of this Organization. When using shared Kafka messaging system across multiple Organizations, this value needs to be unique to each Organization. **Note**: This value is case sensitive and cannot contain any special characters nor spaces, only regular letters and numbers.

UAM

Reserved for future implementation of **User Access Management**, do not input values in this tab.

Application-Specific Tabs

Each package imported in ICMS may have its own settings exposed in application-specific tab.

Consult **ICMS Installation AddOn** document of every package part of each Organization for any package-specific settings that need to be configured in its application-specific tab.

Additional Settings (Optional)

Dependencies

The **ICMS** framework supports the possibility for each component to define dependencies on either additional components that it needs to install/execute, or on other **ICMS** components that are required for proper operation.

LocalPreInstall is a low-level dependency by which a component is requesting the **ICMS** to pre-install some other supporting component **before** installing the actual Landis+Gyr product component itself. A **LocalPreInstall** dependency during an upgrade will result in ICMS simply making sure the supporting component is installed and available on that server, which in most cases does not end up being time consuming beyond the script making sure the dependency exists. A good example of a **LocalPreInstall** dependency would be that the **EmergeApp** component has a dependency on **IIS** and **MSMQ** being available on the target server; this would be presented as two **LocalPreInstall** dependencies in the **EmergeApp** component. During the first server installation, IIS and MSMQ would be installed, while during any upgrades ICMS will simply make sure they still exist. Interestingly, should newer component require modifications in some **LocalPreInstall** dependencies, the difference would be applied to the server during the component upgrade. **LocalPreInstall** dependencies are delivered as a collection of components in pre-requisite packages for either Windows or Linux.

Global is a higher-level dependency that dictates that any specific Landis+Gyr component may require another Landis+Gyr component to exist somewhere in the Organization before installing this one. A good example of a **Global** dependency would be that the **EmergeApp** component has a dependency on **EmergeDb** being available in the Organization before **EmergeApp** can be installed; this would be presented as a **Global** dependency in the **EmergeApp** component.

Detailed Settings

Each **ICMS** component requires a collection of detailed settings (sometimes referred to as **Tokens**) to be defined for proper installation. While many of these **Tokens** are exposed through various tabs in the **Settings**, more are defined for some components, which allow manual overrides of some settings to be applied at various steps of the installation process. The most common override is the **Profile Override**, for which the overall procedure is presented in "Profile Overrides" on page 42. Only exposed **Tokens** can be adjusted for each component.

➡️ *IMPORTANT: Token manipulations are NOT recommended beyond overrides defined by Landis+Gyr within the component installation procedure. These advanced settings are mostly reserved for Landis+Gyr internal use. This is presented here for information and convenience only.*

Figure 4 - 9 on page 53 demonstrates some of the tokens defined for the **CCApp** component.

Figure 4 - 9. Token Example
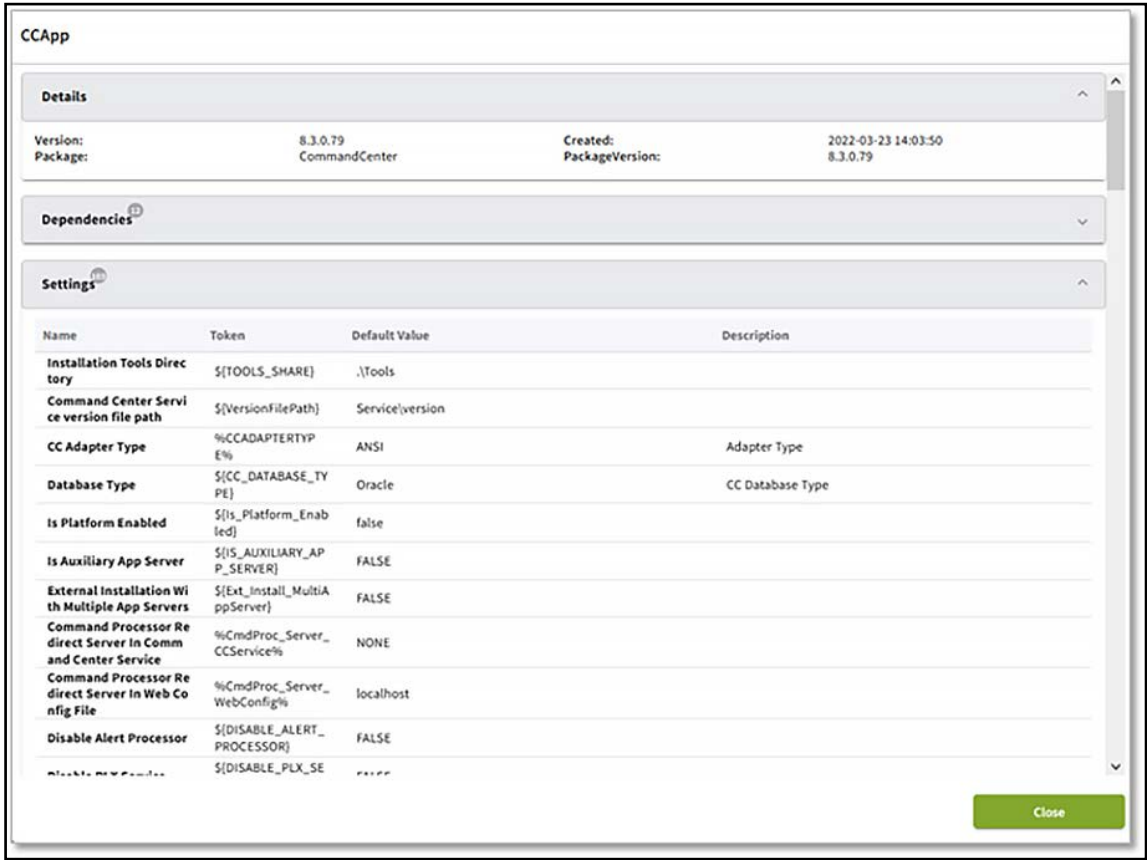
Viewing Dependencies and Detailed Settings

To view dependencies and detailed settings defined for each component, select **Packages** from the side ribbon. From this list, select the **Package** to expand it and see the list of components. Select the component to inspect and the panel on the right will present all the component information including all dependencies and detailed settings.

5
Installation Workflow

Precautions Before Upgrading Emerge

Pre-Upgrade - Emerge Workflow Processes

Before Emerge is upgraded, consideration should be given to some internal processes, to prevent erroneous behavior after upgrade is completed. For the following points, execution may vary with each version of the HES, so details are omitted here since it is expected that users would know how to perform them. Should clarifications be required, contact your Landis+Gyr representative.

- **Broadcasts**. From an operational standpoint, there should be no ongoing broadcasts during an upgrade task. Ensure that no firmware broadcasts are initiated one week before planned upgrade date, and also that no broadcasts tasks are suspended.

- **Gap Detection**. 36 hours before upgrade date, disable Gap Detection on every enabled Gap Detection feature for both reads and/or events.

- **Gap Reconciliation**. One hour before upgrade date and time, disable Gap Reconciliation Retry processes for every enabled Gap Detection feature for both reads and/or events.

- **Gap Reconciliation Retry**.One hour before upgrade date and time, disable Gap Reconciliation Retry processes for every enabled Gap Detection feature for both reads and/or events.

ⓘ **NOTE:** If there is a possibility that your Emerge be still processing Gap Retries when upgrade starts, contact Landis+Gyr to obtain a script to cancel outstanding Gap retries.

Pre-Upgrade - Folder Maintenance

⚠️ **WARNING: The Emerge installer will visit the installation folder during one step of the installation process of every application server. Should there be a large quantity of files in any sub folders in that location, the Emerge installer will require a very long time to complete some tasks and this will negatively impact the installation time of the application.**

Please consult following sub-sections for specific folder maintenance activities.

Queue Data Inspection

Locate the `QueueData` folder. This folder location can be found in Emerge by visiting page **Setup > System Settings**, under the **General Settings** section, and looking for Base Queue File Path.
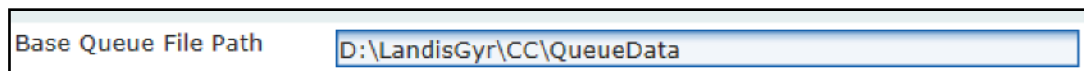
Base Queue File Path	D:\LandisGyr\CC\QueueData

Figure 5 - 1. System Setting - Base Queue File Path

If files in this location cannot be reprocessed for any reason before an upgrade, please discard folder content to prevent upgrade problems.

As a good practice, one should make sure the Base Queue File Path remains empty or nearly empty, by re-processing failed messages on a regular basis. Please contact your Landis+Gyr representative if you are experiencing difficulties with this procedure.

Log File Cleanup

Ensure that number of log files is kept to a minimum. Especially if collector communication logging was enabled, this creates a very large quantity of log files in **TOP** folders.

⚠️ **WARNING: Some installation scripts will enumerate all files under the base installation folder for validation. Having a large amount of log files can prolong the execution of these scripts to excessive duration.**

Pre-Upgrade Quiesce Field Communications

When ready to perform an upgrade, the very first step required is to quiesce all field communications to prevent inbound data from flowing into the system while the upgrade is being performed.

This must be performed outside of Emerge servers, either by closing firewall ports or disabling load balancer Virtual Servers.

ⓘ **NOTE:** Please make sure to test your selected method to quiesce field communications before upgrading.

✳️ **CAUTION: Simply disabling some Emerge and/or Adapters processors is <u>NOT</u> a reliable method of blocking field communications.**

⇨ *IMPORTANT: For Organizations using **RF Mesh IP** and/or **M2M** technology, it might be possible to use the **Store and Forward** feature to accumulate data during an upgrade and thus minimize data loss. Refer to document 98-2548 for eligibility and utilization details of **Store and Forward** package.*

Post-Upgrade - HES Workflow Processes

After an upgrade is completed, wait until data backlog accumulated during planned maintenance window has been processed. Once the overall system has resumed its normal operation and no data backlog remain to process, it is safe to re-enable **Gap Detection** features and **Gap Reconciliation** and **Retry** processes as disabled previously.

Workflow Overview

All workflows of **ICMS** are driven by the **Dashboard** of the **CIN-UI**. Select the **Dashboard** button of the side ribbon to get started with any workflow.
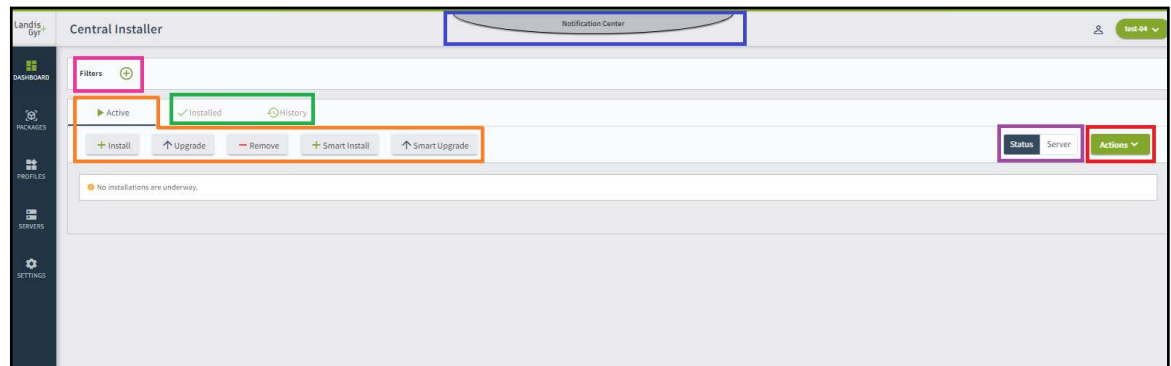

Figure 5 - 2. Dashboard

Workflow controls

These options control the installation workflow starting point. From here the CIN operator can initiate the following workflows on the Organization:

- **Install** profiles to servers
- **Upgrade** servers from existing profiles to new ones
- **Remove** existing profiles from servers
- Perform **Smart Upgrade** to the Organization
- **Smart Install** is a new feature that is being developed and future documentation will explain how to use it.

Notification Center

The **Notification Center** will contain progress and error messages published by the ICMS service, for easy access in the CIN-UI.

Click on the **Notification Center** tab to expose messages, click again on its tab symbol to hide.

Actions controls

These controls allow the workflows to transition to the next state. These are activated by the CIN operator, although some are integrated in various workflow steps for convenience.

- **Check Dependencies** enables the validation of profile selections against product dependencies built-in to **ICMS** components and packages. This step is part of the **Install** workflow for convenience.
- **Prepare…** action is used after profile assignment to server(s). This step of the workflow will assemble each installation package, compress and upload it to the assigned server(s). Server **Prepare…** action can be executed well before the actual installation takes place, to further reduce the maintenance window of the Organization during an installation or an upgrade.
- **Apply…** action will trigger each server to actually perform the installation of each package uploaded during the **Prepare…** activity. On each server, the installation of each package is executed by the **IAS** service.

- **Remove…** action is only available from the **Installed** tab. This action will trigger the removal process of any profiles assigned to any server.

- **Terminate…** action allows to clean up the dashboard to remove a failed workflow. In any of the previous actions, should something cause a failure, the workflow will be halted and displayed on the dashboard for analysis, but a new workflow cannot be re-initiated until the existing one is terminated first. Terminating a workflow will remove all packages uploaded to corresponding server(s) and remove any further workflow traces in the ICMS itself so a new workflow can be restarted after the problem identified in previous failure has been resolved.

View controls

Toggles the dashboard view from a workflow status view to a server-centric view.

Filter controls

Use filters to customize the displayed activities on the dashboard. Filters can be profile-oriented or server-oriented, and many filters can be combined as desired.

Status controls

From these tabs, **CIN** operator can view:

- ✓ **Installed** components of the Organization, with corresponding date. From the ✓ **Installed** tab, the only Actions⌄ available is **Remove…** to remove an applied profile from any server.

- 🕐 **History** of all profiles installed and removed from any server of the Organization, with corresponding date.

Installation

Before performing an ICMS-based installation or upgrade, make sure the **IAS** service is enabled and running on all servers of the Organization.

⇨ *IMPORTANT: For Organizations where Kafka messaging system is required, it is necessary to proceed to installation or upgrade of Kafka components first, including loading topics corresponding to this version of Emerge. Failure to do so will result in improper component start-up for all client services that require Kafka. See ICMS Installation Add-On: Kafka Messaging System, publication number 98-2305, for details.*

New Organization

To perform installation on a new Organization, use the following sequence, from the **Dashboard** of **CIN-UI**.

DB Profile(s)

1. From the ▶Active tab, click **Install**.
2. Select DB-related profile, click **Next**.

3. Select the server from the Organization that will be used to run the DB script part of that profile. Keep in mind, the DB profiles are not expected to be executed directly on DB server, as previously indicated. Click **Next**.

4. Confirm the profile to server assignment from the list, and click **Assign** to proceed.

5. The next panel will summarize the profile assignment to specified server. If ready to proceed with package deployment to server(s), make sure option **Prepare assigned profiles** is selected, and click **Prepare**.

> **(i)** **NOTE:** At this point, the **Dashboard** contains the workflow, with a status of **Dependencies checked**. The workflow can either continue from the current activity or from the **Dashboard** later.

6. The **CIN-UI** will come back to the **Dashboard** and **ICMS** will prepare and send profile package(s) to assigned server(s). Progress can be observed by clicking on the workflow to expand it.

7. After Preparation action is completed:

    a. Click Actions⌄ and select **Apply...**

    b. Select the check box next to the DB workflow to apply.

> **(i)** **NOTE:** There is one workflow per server

    c. Make sure option **Auto apply global dependencies** is selected.

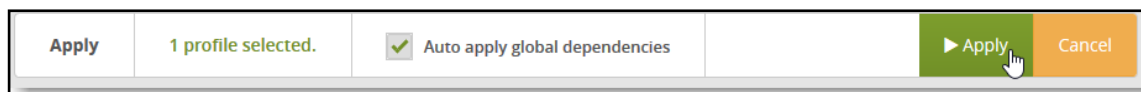   d. Start installation by clicking ▶Apply .

Figure 5 - 3. Apply

8. Installation progress can be observed by clicking on the workflow to expand it. Once installation is complete the workflow will be removed from ▶Active tab and will now show in the ✓ **Installed** and ⊕ **History** tabs.

If using multiple DB profiles, repeat the above sequence so it is orchestrated in such a way that the DB profile of a Landis+Gyr product would be applied before the profile(s) containing the corresponding application components can be applied.

Application Profile(s)

> **⇨** **IMPORTANT:** *If there are any user sessions on any server that are using **Server Manager**, the installation process will fail on them because of locking mechanisms. It is recommended that no user session remain "logged on" to any servers during the installation process.*

After corresponding DB component is successfully applied, application profiles can be deployed to the Organization.

1. From the ▶Active tab, click **Install**.

2. Select ONE application profile, click **Next**.

3. From the server list, select all server(s) where the profile will be applied. Click **Next**.

4. Confirm the profile to server assignment from the list, and click **Assign** to proceed.

5. The next panel will summarize the profile assignment to specified server(s). If ready to proceed with package deployment to server(s), make sure option **Prepare assigned profiles** is selected, and click **Prepare**.

ⓘ

NOTE: At this point, the **Dashboard** contains the workflow, with a status of **Dependencies checked**. The workflow can either continue from the current activity or from the **Dashboard** later.

6. The **CIN-UI** will come back to the **Dashboard** and **ICMS** will prepare and send profile package(s) to assigned server(s). Progress can be observed by clicking on the workflow to expand it.

At this point the CIN operator has two choices to complete the installation:

-   **Prepare all**: Repeat the above process for all application profiles and servers, then **Apply** all application workflows at once or in groups

...or...

-   **Sequenced**: Finalize installation of current profile and apply it to Organization before starting a new one.

Each of the above strategies will work, but the Prepare all scenario can drastically shorten the actual installation process (and thus maintenance window during an upgrade) because the preparation workflows can be completed days ahead of time, so the actual installation consists of applying pre-prepared workflows.

The actual workflow installation is completed as follows in either strategies.

7. After the **Prepare…** action is completed and workflow is in **Preparation complete** status:

a. Click Actions⌄ and select **Apply…**

b. Select the check box next to the application Profile workflow.

ⓘ

NOTE: There is one workflow per server; if profile is assigned to multiple servers, then select all corresponding workflows from the list.

c. Make sure option **Auto apply global dependencies** is selected.
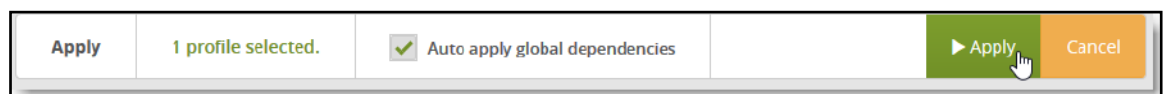
d. Start installation by clicking ▶Apply .

Figure 5 - 4. Apply

8. Installation progress can be observed by clicking on the workflow to expand it. Once installation is complete the workflow will be removed from the ▶Active tab and will now show in the ✓ **Installed** and ◷ **History** tabs.

⇨   **IMPORTANT:** *The ICMS framework is based on components dependencies to establish priority of operations. In this context, it is possible to get all DB and Application profiles to* **Preparation complete** *workflow status.*

At this point, start installation of all DB workflows as described above. Once a DB installation workflow is completed, profiles workflows with components having dependencies on this DB profile will automatically start their own installation process.

Upgrade Existing Organization

.NET Temp Files Cleanup

Most of Emerge components are using .NET framework to operate. It has been observed that in some cases, older temporary files from previous product versions could be remaining in a .NET temporary folder and create problems after a product upgrade. As additional precaution, Landis+Gyr recommends performing the following on each Windows-based server before a product upgrade:

1. Stop all **App Pools** related to Landis+Gyr products

2. Navigate to folder **C:\Windows\Microsoft.NET\Framework64\v4.0.30319\Temporary ASP.NET File**s

3. Delete every file and folder in this location. They will be recreated after product is upgraded and new components are starting up.

ⓘ   **NOTE:** most ICMS packages will perform this cleanup operation automatically during installation; this is presented here for convenience in case cleanup needs to be performed manually.

Cloned Profiles

If using cloned profiles to upgrade an Organization, perform following steps, from the **CIN-UI Dashboard**.

1. From the ▶Active tab, click ⬆Upgrade .

2. Select the existing **DB** profile to upgrade, click **Next**.

3. Select the replacing profile (cloned earlier) of the new product version, click **Next**.

4. Assign the profile to same server (preferred) as previous **DB** profile, and from this point follow the regular installation workflow to deploy DB profile. Two workflows will be created on **Dashboard**: a removal and an installation workflow..

If using multiple DB profiles, repeat the above sequence so it is orchestrated in such a way that the DB profile of a Landis+Gyr product would be applied before the profile(s) containing the corresponding application components can be applied.

Once DB profile(s) are applied, continue with Application profiles.

5. From the ▶Active tab, click ⬆Upgrade .

6. Select ONE existing application profile to upgrade, click **Next**.

7. Select the replacing profile (cloned earlier) of the new product version, click **Next**.

8. Assign the profile to same server(s) as existing profile, and from this point follow the regular installation workflow to deploy the application profile. Two workflows will be created on **Dashboard** for each server: a removal and an installation workflow.

Repeat steps 5 to 8 for each Application profile of the Organization.

Smart Upgrade

ⓘ **NOTE:** If using the **Encrypt and Save** confidentiality settings for the Organization, it is mandatory to visit the **Settings** page and input the Organization protection password before the **Smart Upgrade** feature can be used.

If using the **Smart Upgrade** feature to upgrade an Organization, perform following steps, from the **CIN-UI Dashboard**.

1. From the ▶Active tab, click ⬆Smart Upgrade and follow workflow.

⇨ *IMPORTANT: Should any newer components present different/additional settings from its predecessor, associated profiles will NOT be automatically selected by the Smart Upgrade process. It is possible to review the differences in these settings by selecting the numbered icon next to this component indicating how many settings are different in the new component. This will bring a popup window where changes can be reviewed. If changes are acceptable, select the profiles manually and proceed with installation. If settings need to be revised, it is still possible to use Smart Upgrade in this context:*

*1. Start **Smart Upgrade** and select desired profiles, but at the bottom of the selection panel, click on option **Copy Setting**. This will unselect all following steps and instruct ICMS to create new profiles and thus expose all new settings of the components on the **Settings** tab.*
*2. Visit the **Settings** tab and revisit all settings values, adjusting them as per this and Add-On documents.*
*3. Use **Smart Upgrade** again for these same profiles and this time allow all the steps to execute. Newly adjusted settings from the latest components versions will be applied.*

The **Smart Upgrade** feature will automatically create a new profile based on updated version number of newly imported packages and maintain all existing profile settings and overrides. The new profile auto-generation will locate the last underscore (_) character from the end of the profile name and append updated version number right after.

Server-Level Overrides

In some cases, it is necessary to apply a setting override but specific to a server, not a profile. The procedure to apply a server-level override is as follows.

1. Create profile and assign default values in Settings for all components.

2. In the Dashboard, select + **Install** or ⬆ **Upgrade** action, select required profile(s) where server-level override will be required, and select corresponding servers. See Figure 5 - 5. Click **Assign** button.
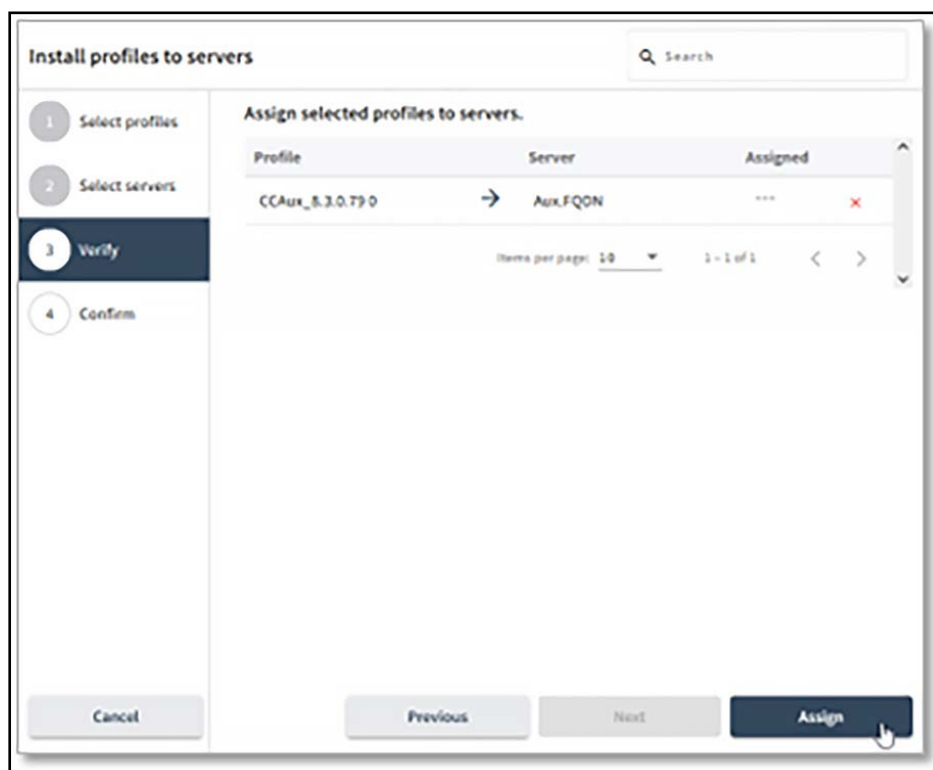
Figure 5 - 5. Assign Selected Profiles

3. On next wizard page, do not proceed with the **Prepare** button, click **Close** button.
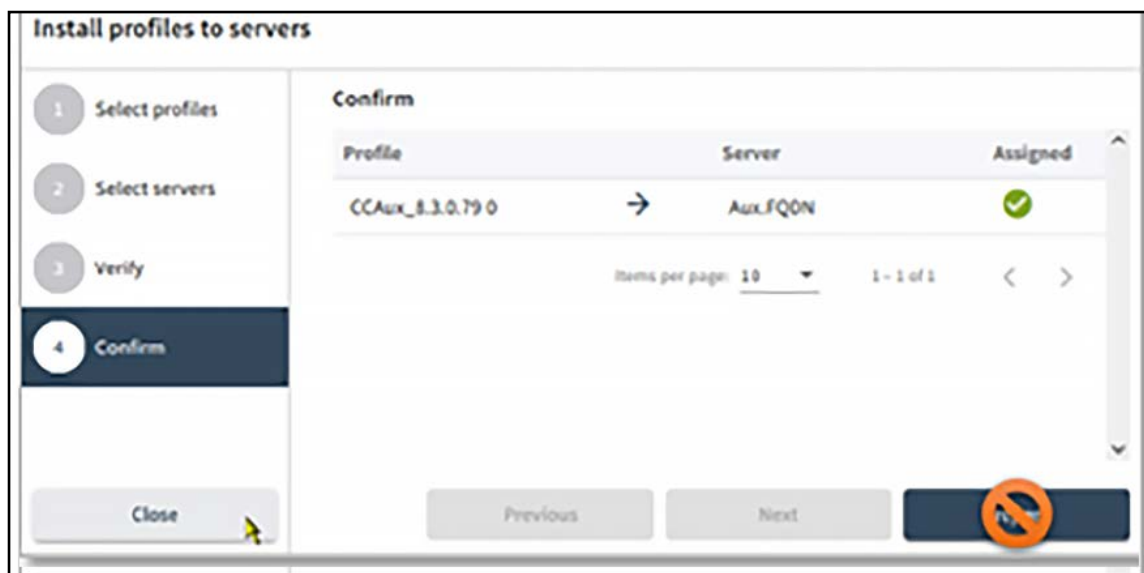
Figure 5 - 6. Do Not Prepare Assigned Profiles

4. Select the **Server** button on the left navigation bar, and for each server where a profile was just Assigned, repeat the following sequence:

    a. Locate server in the list, and then click on it.

b. From the **information** panel on the right, and then click **Component Settings**.

Figure 5 - 7. Component Settings

c. From the next list, select the component for which a setting override is required.

Figure 5 - 8. Component Settings Override

d. Locate the setting(s) for which the server-level override is needed, and update setting to desired value in the **Override Value** input box. You can use the search bar.

Figure 5 - 9. Override Value

    e. Change setting to desired value, and press Apply Settings button.The component list will now indicate overrides applied at server level.
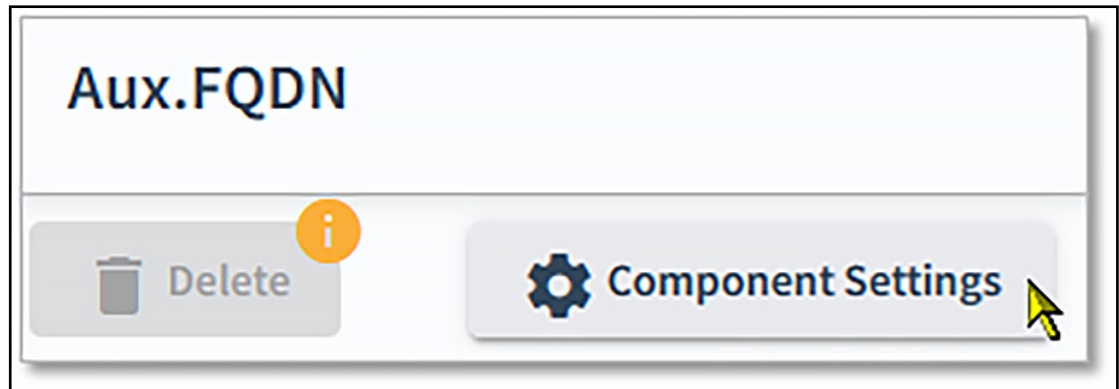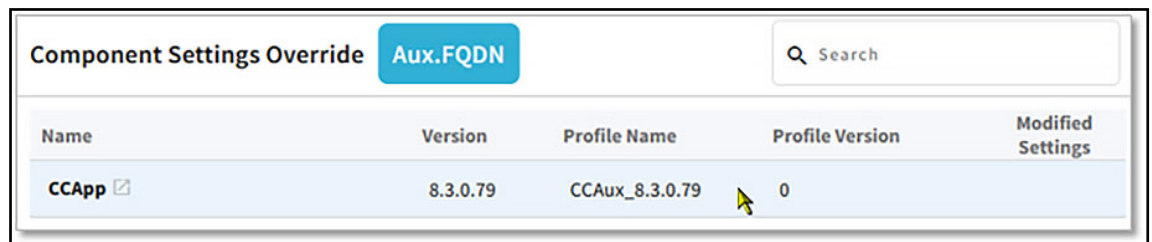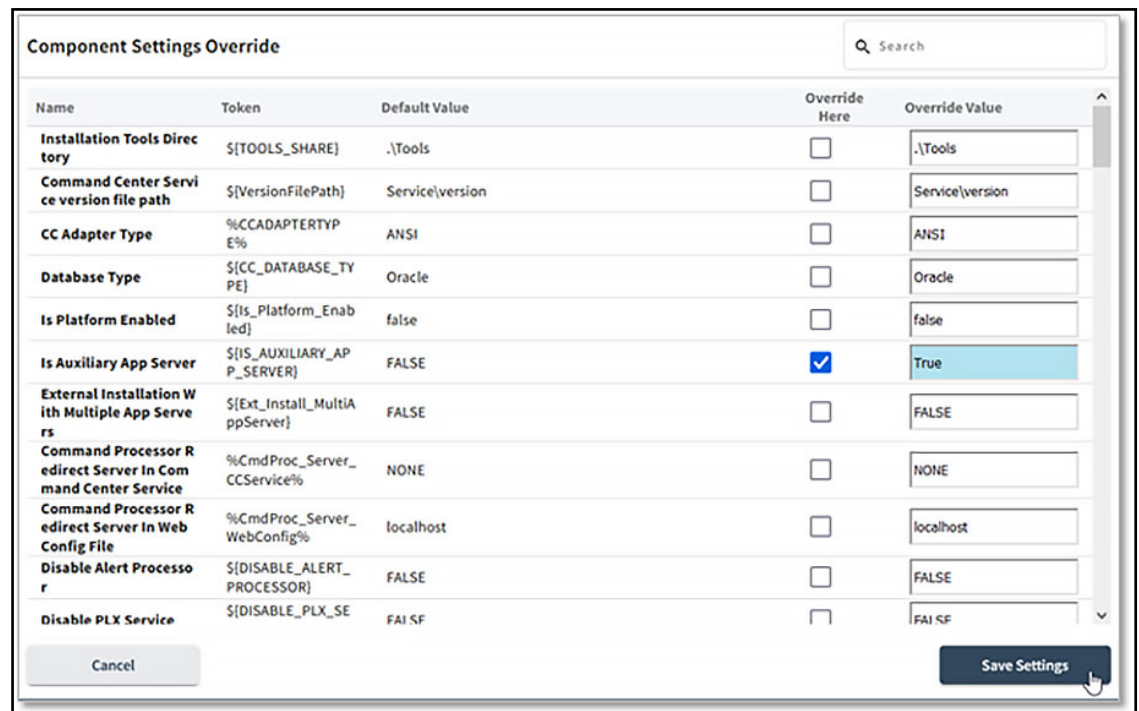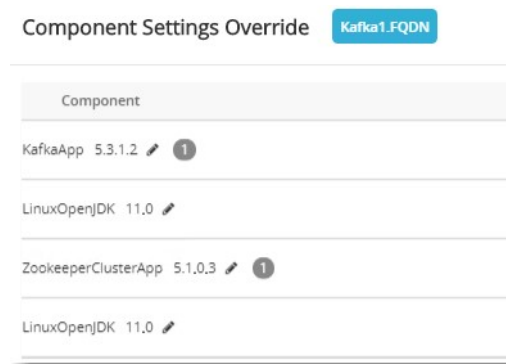

Figure 5 - 10. Component Settings Override

    f. Repeat steps c-d-e above for any other component where server-level overrides are needed for this server.

    g. Click **Close** to accept all server-level overrides.

5. Back to the **Dashboard**, installation or upgrade can now continue by **Preparing** and **Applying** the updated profiles.

Clean Up

After upgrading an Organization, the **ICMS** may contain unused **Profiles** and may even contain application packages that are no longer required by any Organizations managed by this **CIN** server. Remove all of these to keep the **ICMS** database to the smaller possible size and free up disk space.

Automatic Cleanup

Select **Packages** from the side ribbon. Select **Delete all packages**, this will automatically remove all packages no longer used by any organization as well as all profiles unused in the current Organization.

Manual Cleanup

1. Start by removing **Profiles** by clicking **Profiles** on the side ribbon, and for each unused **Profile**, select it, verify it is marked as *Not In Use* then click **Delete**.

2. Finish maintenance by removing obsolete packages by clicking **Packages** on the side ribbon; from the list, any package not assigned to any profile will be displaying an active garbage canicon, click it to remove the package.

Disable IAS

For production Organization deployments, it is recommended to stop and disable the **IAS** service on every Organization server, until further maintenance window is required in the Organization

6

Non-ICMS Product Installation

Overview

For this version of Emerge, there are currently no components that do not support ICMS-based installation.

7
Post Installation

One-Time Only Server Configurations

After first installation of packages on a new server, some post-installation steps may be required.

Consult **ICMS Installation Add-On** document of every package part of each Organization for any package-specific adjustments.

The following are applicable to most packages and are presented here for convenience. They are not duplicated in any **ICMS Installation Add-On** documents.

MSMQ Adjustments

If using a dedicated drive for MSMQ, perform the following:

1. Reconfigure MSMQ to use dedicated drive, since default MSMQ installation is on C: drive.

2. Disable MSMQ Quotas.

3. Restart MSMQ service for the changes to take effect.

SSL Bindings

If Organization has a requirement for encrypted communication, add **HTTPS** bindings to the **Default Web Site** in **IIS** on all servers where **HTTPS** is used. On new servers this cannot be done before installation since **IIS** will be installed by **ICMS** and thus is not available at the server preparation step.

For Organizations where components are installed on Linux servers, consult the respective **ICMS Installation Add-On** document for details.

Automated Server Maintenance

Landis+Gyr provides components to automate basic server maintenance, available when using **Windows Prerequisites** and **Linux Prerequisites** packages version 5.x or later.

Components

The following table presents components breakdown:

Component	Role/Definition
Files Cleanup for Windows	Activate scheduled weekly task to automatically clean up all Landis+Gyr components **logs** folders, all old files from poison folders, and optionally **C:\Temp**, designated **Windows temp** and **IIS log** folders.

Component	Role/Definition
Deadletter Queues Cleanup for Windows	Activate scheduled weekly task to automatically clean up all **Deadletter Queues** from MSMQ, including all **System Queues**.
Files Cleanup for Linux	Activate scheduled weekly task to automatically clean up all Landis+Gyr components **log** folders.

Maintenance Settings

Maintenance settings will be exposed on the **Misc** tab in **CIN UI** only when profiles are created containing maintenance components that will be deployed to servers.

Application Settings	Description
Cleanup Logs Enabled	Selecting this option will allow installation of **Files Cleanup for Windows** and/or **Files Cleanup for Linux** components. If not selected. attempting to deploy these components will fail.
Logs Retention Days	Number of days to keep log files. Any files older than this value will be deleted when the cleanup job runs. **Valid values** are from `7` to `95` days. **Default value**: `45 days`. Landis+Gyr recommends a value of 45 days or less.
Cleanup Extra Folders on Windows	When enabled, include additional Windows folders as part of the log cleanup job: • `%TEMP%` • `C:\inetpub\logs (IIS Logs)` • `C:\Temp` **Recommended value**: `Enabled`
Cleanup Deadletter Queues Enabled	Selecting this option will allow installation of **Deadletter Queues Cleanup for Windows** component. If not selected. attempting to deploy this component will fail.

Deployment

To enable any of these features, create profile(s) containing desired component(s) and:

1. Adjust maintenance settings from **CIN UI** (see details below).

2. Deploy profile(s) containing Windows-related component(s) to Windows servers running any Landis+Gyr application components.

3. Deploy profile containing Linux-related component(s) to Linux servers running any Landis+Gyr application components.

On Windows servers, deploying each of these components will add a distinct task in Windows **Task Scheduler**, scheduled for weekly execution on Sunday morning. These tasks will run using SYSTEM user account with elevated privileges.

On Linux servers, deploying each of these components will add a distinct task in **crontab** of root user, scheduled for weekly execution on Sunday morning.

Profile Overrides

Additional adjustments of some settings may help refine desired behavior. It is possible to adjust any of the following settings using a Profile-level override before applying profile to servers.

Component	Setting	Override Description
Files Cleanup for Windows	Cleanup Poison Folders on Windows	Include folders containing Poison messages, if they exist. Enabled by default. Set to **FALSE** to ignore these locations.
Files Cleanup for Windows	Cleanup Task Delete Empty	After deleting old files in a folder, remove the folder itself if it is now empty. Enabled by default. Set to **FALSE** to keep empty logs folders.
Files Cleanup for Linux	Cleanup Logs Job User Account	User account to use to execute the logs cleanup job. Account selected must have sufficient privileges to remove files from all Landis+Gyr components folders. Default value: `root`

After First Installation and Every Upgrade

After every upgrade of packages on a new server, some post-installation steps may be required.

Consult **ICMS Installation Add-On** document of every package part of each Organization for any package-specific adjustments.

The following are applicable to most packages and are presented here for convenience.

App Pools and Services Adjustments

Most packages will include automated App Pools and Services adjustments for all their respective components. If necessary, manually adjust these settings following the information below.

IIS App Pools

On all Windows-based servers, perform the following in the IIS manager.

On all Application Pools of the solution, adjust **Advanced Properties** as follows:

- Identity > Network Service (optional, for server hardening only)
- Idle time out > zero
- Recycling regular time > zero
- Recycling Specific Time Span > between 22:00 and 23:50

ⓘ **NOTE:** Recycling time of every Application Pool on the same server should all be different. Landis+Gyr recommends a minimum delay of two or three minutes between each Application Pool recycling time. No Application Pool recycling time should be set past 23:50 to ensure recycling is completed before midnight.

Windows Services Adjustments

Every Windows service of the Emerge solution can be configured with automatic recovery settings. Perform the following steps from the **Services** snap-in for every service where this configuration is desired:

1. From the Open **Server Manager**.

2. Right-click on the service name where recovery services needs to be configured, select **Properties** to display the Properties window.

3. In the **Recovery** tab, ensure that the indicated settings are as shown.
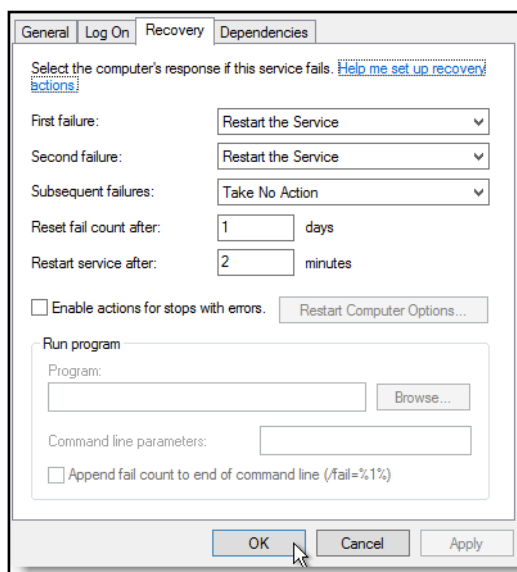
Figure 7 - 1. Recovery Tab

(i)   **NOTE:** Adjust the **Reset fail count after value** to 1 to reset the **Service Failure count** on a daily basis. Using a value of 0 will never reset the count

4. Click **Apply > OK** to apply the settings.

SSL Bindings

If the **HTTP Protocol** is defined as **HTTPS** in the **Misc** tab of the CIN UI, security bindings of some packages must be adjusted manually as certificate binding of micro-services cannot be scripted in ICMS packages. Please refer to each Add-On document for details, in the **First Installation and Every Upgrade Version Specific sections of the Post Installation** chapter.

A
Troubleshooting

CIN UI Does Not Show Any Data

Possible Cause

- UI back-end is not configured to connect to ICMS-server

Correction

1. Shutdown the UI.
2. Open **conf/cin-ui.conf** and edit **cin.core.host** and **cin.core.port** to point to the ICMS-location.
3. Start the UI.

Possible Cause

- ICMS is not running.

Correction

1. On the ICMS server, start a **Task Manager** and select **Services** tab.
2. Find **LGInstallationConfMgmtSvc**.

   a. Start **LGInstallationConfMgmtSvc** if it is not already running.

   b. Restart **LGInstallationConfMgmtSvc** if it is running.

Possible Cause

- ICMS data migration failed with error.

Correction

1. Analyze the error to identify the root cause of the failure. in most cases failure can be observed as:

   a. Erroneous SQL Server information entered (verify instance, FQDN, port)

   b. Invalid SQL account credentials used.

2. Connect to the SQL database / instance and:

   a. Delete the ICMS database.

   b. Delete the ICMSUser.

3. Re-execute the ICMS .MSI file from elevated DOS prompt, if previous ICMS installation completed successfully, this will uninstall existing ICMS service. If previous ICMS installation did not completed at all, this will trigger a new installation. Follow step 5 below.

4. Re-execute the ICMS .MSI file from elevated DOS prompt, making sure to use updated information where needed.

Possible Cause

- ICMS data migration completed but no Organization data is showing in CIN UI after ICMS upgrade.

Correction

1. This usually happens when wrong **ICMS Files Dir** location was entered (not same as previous installation) when executing the ICMS installation wizard, resulting in no Organization data being migrated to the SQL Database. Inspect all drives on the CIN server and look in **\ICMSFiles\ICMSDataStore** location for XML files corresponding to Organizations that existed in previous ICMS database. Note the full path in the form **D:\ICMSFiles** where **D:** would be the actual drive letter where XML files were found.

2. Connect to the SQL database / instance and:

   a. Delete the ICMS database.

   b. Delete the ICMSUser.

3. Re-execute the ICMS .MSI file from elevated DOS prompt, if previous ICMS installation completed successfully, this will uninstall existing ICMS service.

4. Re-execute the ICMS .MSI file from elevated DOS prompt, making sure to use adequate value for **ICMS Files Dir** as found in step 1 above.

CIN UI Does Not Refresh

The **CINUI** should automatically refresh pages as the **ICMS** performs background tasks. If the **CIN-UI** pages do not auto-refresh,

Possible Cause

1. The **CINUI Port** configured in the **ICMS** during ICMS installation is not consistent with the **CINUI Port** configured in the **CINUI** during CINUI installation.

Correction

Re-install ICMS with proper CINUI Port information.

...or......

Edit the ICMS config file **D:\LandisGyr\ICMS\LGInstallationConfMgtSvc\LandisGyr.ICMS.Service.exe.config** and set the value of key **cinUIApiGatewayPort** to the proper **CINUI Port** value. Restart ICMS service.

Logfiles

Logfiles path of a specific profile and components can be found in the profile information in the UI. Links can be clicked to see the installation status or any error message.

Installation Error

If a workflow comes to fail during its execution, perform the following activities:

1. From **CIN-UI Dashboard**, expand the failed workflow, and from the list of activities locate the one in error.

2. Click on the component that errored out to expand it, then select the hyper link for the **Log File**.

3. Analyze error documented in the log file and resolve the problem. It could be necessary in some cases to consult the actual installation package of the failed component. From the failed component section, take note of the **Guid** value. Connect to the target server where failure occurred, and navigate to **D:\IASFiles\<Instance>** folder. In there one sub-folder will be named same as the **Guid**, visit the folder and analyze the scripts as needed.

4. From **CIN-UI** expand the Actions list and select the **Terminate…** option; select the failed workflow to terminate it and click **Terminate**.

5. Restart workflow as a new profile deployment even though it might have failed as an upgrade workflow (because an upgrade starts with a Remove workflow)

Repeat for all failed workflows.

Wrong Settings

After deploying an Organization, it is possible to realize some settings were not configured properly. If this happens, perform the following activities.

1. Fix the erroneous settings to their proper value. Note all components related to the setting.

2. Select **Profile** button from the side ribbon; from the profile list note all **Profiles** that contain identified components from previous step.

3. From **CIN-UI Dashboard**, select Installed tab; expand the Actions list and select the **Remove…** option.

4. From the list, work one profile at a time.

   a. Select all workflows of one profile that need to be re-applied.

   b. Select ⁻Remove to initiate the removal workflow

   c. Select all servers where this profile is applied.

> **NOTE:** Selecting workflows from different profiles in the same operation will trigger removal of the sum of all components of all selected profiles from all servers selected; as a result the removal will attempt to remove components from servers where they were not installed. This is not recommended.

   d. Repeat step 4 for every profile where an erroneous setting might have been used.

   e. For each removed profile, restart the regular installation workflow as a new profile deployment even though it might have been applied as an upgrade workflow.

B
Antivirus Exclusions

Background

Antivirus programs of all kinds constantly scan folders and files for changes. This takes CPU cycles and imposes additional disk activities, and when not implemented carefully, will make a good system come to a crawl by locking files and folders during scanning when other processes are trying to access them during their regular operations.

Over time, Microsoft published their own documentation about Antivirus exclusions that coincides 100% with Landis+Gyr findings. In terms of Linux servers, McAfee and Symantec have both published papers on the very same topic, which we bring back here as our own recommendation as well. An additional package has been added to the list since it is a transactional component similar to MSMQ and thus replicating on Linux the Microsoft recommendation in that respect.

In terms of our own products, we recommend excluding our base installation folder so our processes, services, and application pools have free access to their DLLs, config files, log folders, etc., without any hindrance from a virus scanning program. Viruses and malware propagate to system folders in general, that will be protected by the Antivirus program.

Below are details for each operating system.

Windows Servers

The Windows exclusion list includes the following folders/files:

- `C:\pagefile.sys` or all disk drives / locations where any active `pagefile.sys` system file exists.
- `C:\inetpub\logs\LogFiles\W3SVC1` or any custom location defined for IIS logs.
- `%SystemRoot%\SoftwareDistribution\Datastore`
- `%SystemRoot%\SoftwareDistribution\Datastore\Logs`
- `%SystemRoot%\Security\Database`
- `%AllUsersProfile%\NTUser.pol`
- `%SystemRoot%\System32\GroupPolicy\`
- any `Registry.pol` file located under any sub-folders from this one
- `%windir%\Microsoft.NET\Framework\v4.0.30319\Config` folder, files `web.config` and `machine.config`
- `%windir%\Microsoft.NET\Framework64\v4.0.30319\Config` folder, files `web.config` and `machine.config`
- `%SystemRoot%\system32\msmq\storage` or any custom location defined for MSMQ storage

In some cases, the **GroupPolicy** and **GroupPolicyUsers** folders may not contain the **registry.pol** file. It all depends on how policies are implemented on each server. Also, if MSMQ was configured to use storage in a different location, the exclusions must be adjusted accordingly. All the above are also consistent with Microsoft guidelines as found here:

https://support.microsoft.com/en-us/kb/822158

The Landis+Gyr product exclusion list includes:

- `D:\LandisGyr`

  ...or...

  The base installation folder for all Emerge-related sub-folders, including crypto-related content, where applicable. If there is no common root folder for installation, include every folder where Emerge, Gridstream Integration Suite, Emerge Extensions (RF Mesh IP, M2M, PANA, etc.), and Crypto client components are installed.

- On ICMS server: `D:\ICMSFiles` ...or... the value designated as **ICMS Files Dir** used while installing **ICMS** service

- On all other servers: `D:\IASFiles` ...or... the value designated as **IAS Files Dir** used while installing **IASWindows** installation agent service

CAUTION: Some Landis+Gyr services may create / change config files during their registration process, this is normal and must be allowed.

WARNING: No anti-virus or anti-malware software installed on any servers hosting any Emerge components should be allowed to tamper with access URLs, HTTP headers, inject cookies, or perform any other manipulations on any access methods and/or processes.

NOTE: McAfee recommends using version v5.0 Patch 6 (i.e. 5.0.6 build 220 or 5.0.6.22) or newer. Using older version can create scanning problems with IIS worker threads. Testing using this version was completed by McAfee and not Landis+Gyr. Landis+Gyr does not recommend any particular antivirus product.

Linux Servers

The Linux basic exclusions are:

- **/sys**
- **/proc**

Additional reference material may be reviewed at [McAfee](#) and [Symantec](#).

Landis+Gyr components distributed as ICMS packages will use the following locations, which should be excluded from on-access scanning:

- **/opt/landisgyr**
- **/opt/kafka**
- **/etc/landisgyr**
- **/var/log/landisgyr**
- **/var/log/kafka**
- **/var/log/zookeeper**
- All folders designated for Kafka and Zookeeper data, see *ICMS Installation Add-On: Kafka Messaging System Adapter Installation Package Specifics*, 98-2305, for details

Tunnel Manager component makes use of Beanstalk for queue management, so the following must be excluded as well:

- **/var/lib/beanstalkd/bin**
- **/var/lib/beanstalkd/log**

C
Database Application Accounts Password Rotation

Using ICMS for DB Passwords Management

Landis+Gyr recognizes the need for customers to perform periodic changes to account credentials used by applications to access database information.

Many packages published with Emerge 2.0 now provide a component that allows updating the database connection string on each server without re-installing the application component.

These components will be listed in their respective package as:

<ComponentApp>UpdateCSonly

or

<ComponentApp>UpdateConnectionStringOnly

> **CAUTION:** If a component uses a database application account and does not support this procedure for DB application password rotation, consult the component's own ICMS Add-On document for details related to DB application password changes.

DB Password Rotation Procedure

To proceed with a database application password rotation, Landis+Gyr recommends initiating a Emerge downtime to execute the following procedure:

1. From CIN UI, create a profile **UpdateDBAppPasswords** that contains all the components that allow changes to DB connection string from all packages in use within the Organization. This step can be performed before the Emerge downtime.

2. Update all DB related passwords on the **App Databases** tab of the **CIN UI** and save changes.This step can be performed before the Emerge downtime.

3. Quiesce all Windows servers, from the **CIN UI**, apply a **StopAll** profile that contains `StopAll` component, to all Windows servers.

4. Perform the desired password changes in the Database, for all DB application accounts, using same passwords as updated in Step 2 above.

5. Using the **CIN UI**, apply the **UpdateDBAppPasswords** profile to all Windows server. Each component will scan the `machine.config` file and update its respective credentials only if the DB application account is found in the file. The `machine.config` file will automatically be re-encrypted after the operation is completed.

6. If some packages in use within this Organization do NOT have the component to update the connection string from the **CIN UI**, proceed with manual changes to the connection string on all servers where these components are installed.

7. Using the **CIN UI**, proceed to remove the **StopAll** profile from all Windows servers.

> **NOTE:** Landis+Gyr can provide the detailed procedure to manually change DB application account passwords in the connection string of the `machine.config` on Windows servers. Consult your Landis+Gyr representative for details.