# Predictive Routing Deployment and Operations Guide

## AI Core Services Single-Host Deployment

4/2/2026

# Contents

# AI Core Services Single-Host Deployment

AI Core Services (AICS) is deployed using Docker containers on hosts running Docker Service. It is required that you deploy Docker Service in your environment, and Genesys provides the AICS installation file, which includes the multiple Docker images packaged as .tgz files. These images are loaded to the Docker Engine during the installation phase and are started in the desired pattern to ensure services are configured properly.

> ### Warning
> The instructions on the majority of this topic are intended only for **new deployments**. In particular, do not run the **start.sh -I** script if you have an existing version of Predictive Routing running in your environment. It will clear all existing data from your database and would result in data loss. *To upgrade an existing deployment of Predictive Routing*, following the instructions in Install into an Existing AICS Deployment.

## Target Server Requirements and Recommendations

You must have the prerequisite hardware and software available and have performed the necessary preliminary steps to install and start Docker before installing AICS. Note that some of the steps require **sudo** access to the target servers.

- For hardware and software prerequisites, see AICS Prerequisites.
- You must have at least 50 GB free disk space on your root partition. For complete sizing requirements, see the sizing worksheet linked from Sizing for Premise Deployments.
- The target server cannot be a Docker image. It can be a virtual machine.
- By default, AICS deployed on a single host uses port 443 to be open for access to the API and web application. If you need to change the default port assignment, see Change the Default Port for AICS.
- For faster Dataset uploads (in release 9.0.013.01 and higher) and Agent and Customer Profiles (in release 9.0.015.03 and higher), AICS uses a separate service, which requires that port 9000 be open and accessible to external world on the public IP address of the target server. If port 9000 is not open and available, you can still upload Datasets, but at a reduced upload speed.
- SELinux (Security Enhanced Linux) should be disabled or running in permissive mode. See How to disable SELinux for instructions.

### Preliminary Steps: Install and Start Docker

### Important

- Genesys does not ship Docker as a part of AICS. You must install Docker in your environment before you can load the AICS containers. See AI Core Services system requirements for supported Docker versions.
- You might need an active internet connection to download additional libraries when installing Docker.

1. Install Docker-ee or Docker-ce. Click the desired version to access the relevant deployment instructions on the Docker site.
   A Docker deployment provides a complete self-contained environment, so that you do not need to manually configure ports or address compatibility issues for communication among the Docker containers that comprise AICS. All of that is taken care of ahead of time, and the completed Docker containers work together seamlessly upon deployment.
2. Create a new user to be used for installing and starting AICS. This user must be a member of the **docker** Linux group that you created during the Docker installation process. In most cases, the following set of Linux commands is enough to create the user needed for installing and starting AICS:

   ```
   $ sudo useradd PR_USER
   $ sudo usermod -aG docker PR_USER
   $ sudo usermod -aG systemd-journal PR_USER
   $ sudo passwd PR_USER
   ```

   - You must have **sudo** rights to execute these commands.
   - In the example commands, the user is given as *PR_USER*. You can replace this user name with any valid Unix name. This topic refers throughout to PR_USER; if you choose a different name, substitute that actual name in its place.
3. Grant SSH access to PR_USER so that you can copy the AICS installation package to the target server. The AICS installation package should always be copied to the target server by PR_USER into the PR_USER home directory.
4. To enable the Docker service, execute the following command:

   ```
   $ sudo systemctl enable docker
   ```
5. To start the Docker service, execute the following command:

   ```
   $ sudo service docker start
   ```

## Preliminary Step: Create a Separate Disk for the MongoDB Database

Always use a separate disk partition for storing MongoDB data. This partition should be mounted as `/datadir`. The size of partition depends on your expected data usage, but it must be at least 50 GB. For disk partitioning, use standard Linux tools.

> **Important**
>
> The `/datadir` partition **MUST** exist before you install GPR and the user who is executing the GPR installation should have write access to the partition.

Use the following command to check how much space MongoDB is currently using:

```
$ du -h /datadir
```

In HA scenarios, checking one node is enough because the same data is replicated on all nodes.

## Installing and Configuring AICS

The following instructions are intended only for new installations into a fresh environment. If you have previously installed AICS using Docker containers, see Install into an Existing AICS Deployment.

A fresh AICS installation consists of the following steps:

1. Unzip and Unpack the Repository File
2. Install AICS
3. Initialize the Application
4. Restart the Containers
5. Verify the Installation
6. Set Values for the AICS-Related Configuration Options - some configuration options are mandatory
7. Set Values for Environment Variables - some environment variables are mandatory
8. Configure AICS to Use HTTPS - mandatory
9. Scale the AICS Deployment (jumps to the Scaling AICS topic in this *Guide*)
10. Access the Logs for AICS (jumps to the Logging topic in this *Guide*)
11. Clean Up Disk Space
12. (Optional) Configuring AICS for Large Datasets
13. (Optional) Change the Default Port for AICS
14. (Optional) Turn on SSL for NGINX
15. (Optional) View Container Disc Usage
16. (Optional) Back Up Your Data
17. (Optional) Map a Local Volume to a Container
18. (Optional) Uninstall AICS

> **Important**
>
> - Genesys strongly recommends that you do NOT use the **root** user to install and start AICS. On Linux, the root user should be used only for administrative tasks.
> - You do not need to have **sudo** rights to install and start AICS. **Sudo** rights are required only when executing the preparatory steps documented above.
> - All steps required to install, start, restart, or upgrade AICS should be executed as PR_USER.
> - MongoDB connections among the Workers, MinIO, and Tango containers uses SSL (TLS 2.0).

## Unzip and Unpack the Repository File

1. Copy the **IP_JOptPlatform_<*version_number*>_ENU_dockerlinux.zip** file to the desired installation directory. Genesys recommends that you use the PR_USER home directory as destination for the AICS installation package.
2. Unzip the **IP_JOptPlatform_<*version_number*>_ENU_dockerlinux.zip** file, using the Linux `unzip` command, to access the **IP_JOP_PRR_<*version_number*>_ENU_linux.tar.gz** repository file.
3. To unpack the **IP_JOP_PRR_<*version_number*>_ENU_linux.tar.gz** repository file, execute the following command:

   ```
   $ tar -xvzf IP_JOP_PRR_<version_number>_ENU_linux.tar.gz
   ```

   This creates the **IP_JOP_PRR_<*version_number*>_ENU_linux** directory.

   All bash scripts required to install and operate AICS can be found in the **IP_JOP_PRR_<*version_number*>_ENU_linux/scripts/** directory.

The Predictive Routing scoring engine, API, and web interface are all deployed in a single container, which has the internally-used informal name of Tango.

In addition, Gunicorn `workers_*` containers provide specific functionality, indicated by the container names. The number and functions of the Workers containers differ in some releases. In earlier versions of AICS, many of the functions later allocated to separate Worker containers were performed within the Tango container.

The AICS package also includes various third-party components:

- MongoDB: Stores data needed for scoring agents and making matching predictions.
- NGINX: (The NGINX container was removed in release 9.0.015.03.) A front-end proxy serving content to the Predictive Routing server. Can also be used *in non-production environments only* for load-balancing in multi-server high-availability architectures.
- Gunicorn: A Python WSGI HTTP Server for UNIX, which is a pre-fork worker model. The Gunicorn server is broadly compatible with various web frameworks, simply implemented, light on server resources, and fairly speedy.

- MinIO: Starting in release 9.0.013.01, the MinIO container provides fast dataset uploads and for temporary dataset storage after upload to GPR. In release 9.0.015.03 and higher, Agent Profile and Customer Profile data is also uploaded using MinIO. (Data is stored in MongoDB in the long-term.)

## Install AICS

Perform the installation using PR_USER (or the name you assigned in the Preliminary Steps , above). Installation does not require **sudo** rights and should NOT be done by the root user.

To install AICS, execute the **install.sh** script:

```
$ cd IP_JOP_PRR_<version_number>_ENU_linux/scripts/
bash install.sh
```

If you are managing your MongoDB deployment externally, run the **install.sh** script with the **-externalMongo** flag, as follows:

```
$ bash install.sh -externalMongo
```

The installation script verifies that the target server has sufficient hardware resources. If not, the installation process terminates without performing the install.

The installation script also checks the following:

- Installed Docker package is docker-ce or docker-ee.
- Docker version is supported.
- Number of cores in the server is sufficient.
- Root partition free space is sufficient.
- PR_USER (or your username) belongs to the Docker group..
- PR_USER (or your username) belongs to the systemd-journal group (for container log checking).
- Docker service is running.

## Configure AICS

After installation but *before starting AICS*, perform the following steps:

1. Configure the S3_ENDPOINT environment variable, as explained in Set Values for Environment Variables (below).
2. Ensure that port 9000 is open and available (not blocked by a firewall).

These steps ensure that you can take full advantage of fast dataset uploading provided by MinIO.

## Initialize the Application

Use the following command to initialize the application database and start the application. This command also sets the password for your default user, super_user@genesys.com. Replace the

variable <'my_password'> in the command below with a strong password, and record it securely for future reference.

```
$ cd scripts; bash start.sh -l -p <'my_password'>
```

> **Warning**
> Loading initial data erases any existing data stored in database!

Use the following information to access the Predictive Routing application from a browser:

- **URL:** https://*<server_ip_address>*
- **username:** super_user@genesys.com
- **password:** the password you specified

By default, the AICS installation procedure creates two instances of the model_training worker container and one instance of each of the other worker containers. For a detailed discussion of how and when to scale all the AICS containers, see Scaling AICS.

You can change the number of workers using the following commands:

```
$ cd IP_JOP_PRR_gpr_rc_ENU_linux
$ ./docker-compose -f scripts/docker-compose.yml -p workers scale model_training=4
$ ./docker-compose -f scripts/docker-compose.yml -p workers scale analysis=2
$ ./docker-compose -f scripts/docker-compose.yml -p workers scale purging=2
```

To stop the application run:

```
$ cd scripts; bash stop.sh
```

### Troubleshooting the Initialization Process

If you need to troubleshoot execution of the **start.sh** script:

- Run the following script:

```
$ cd scripts; bash -x start.sh
```

It shows every command executed and the resulting output.

To turn on the DEBUG level of logging:

1. Add the line `LOGLEVEL=DEBUG` to the **conf/tango.env** file
2. Restart the application.

## Restart the Containers

To restart the Docker containers run the **restart.sh** script:

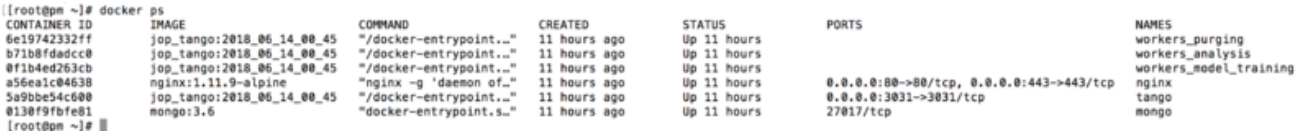
```
$ cd scripts; bash restart.sh
```

## Verify the Installation

To check the status of the containers, run the following command on the target server:

```
$ docker ps
```

You should see output similar to the following:




Check the AICS logs for the various containers, as described in Operations: System Monitoring and Logging .

## Set Values for the AICS-related Configuration Options

AICS-related options are configured on the `Predictive_Route_DataCfg Transaction List` object.

- For descriptions of the options, including default and valid values, see Deploying: Configuration Options .
- For instructions on setting values for configuration options, which is done on the **Configuration** tab of Genesys Administrator Extension, see Configuration Manager in the *Genesys Administrator Extension Help*.

## Set Values for Environment Variables

This section lists environment variables that must or should be configured for optimal GPR performance, and the recommended values. Adjust these values as necessary, based on your specific environment.

> ### Warning
> The **tango.env** file, which contains the environment variables, is overwritten when you perform a software upgrade. Before upgrading, save a copy of the **tango.env** file and refer to it to reset your variables. Note that if you simply overwrite the new **tango.env** file with your existing one, any environment variables added in the new release are removed.

Environment variables are defined in the **IP_JOP_PRR_<*version_number*>_ENU_linux/conf/tango.env** file. The same file is used for both single node and HA deployments.

To add a new variable:

1. Create a new line in the **tango.env** file.
2. Add the variable and its value, using the following format:
   `<NEW_ENV_VAR>=value`

> **Important**
>
> - Do not use quotes for string parameters.
> - Remove trailing spaces.

Changes take effect on restart of the tango container (run the `bash scripts/restart.sh` command command). In an HA environment, with multiple instances of the containers running, restart is performed sequentially (a rolling restart), so that there is no downtime of the GPR application.

### Configurable Environment Variables

- **ADD_CARDINALITIES_EVERY_N_RECORDS** - When you append data to an Agent or Customer Profile via the API, cardinalities are computed only for the appended data portion and only when the number of agents or customers set in the ADD_CARDINALITIES_EVERY_N_RECORDS parameter is reached. The results of computation are added to the already-stored cardinality values. This significantly improves speed when loading new data by avoiding simultaneous recomputations on the full data collection when there are multiple frequent appends done in small batches.enables you to specify how many appended records are added to an Agent or Customer Profile before GPR recalculates cardinalities. The default value is `1000`.
  - Notes:
    - This functionality is available only when you use the Predictive Routing API. If you append using the Predictive Routing application interface, all cardinalities are recalculated.
    - Full automatic computation happens only once, when an Agent or Customer Profile is uploaded the first time for schema discovery.
    - You can force recomputation of cardinalities on the full Agent or Customer Profiles collection using the POST **compute_cardinalities** API endpoint. For details, see the *Predictive Routing API Reference*. (This file requires a password to open it. Contact your Genesys representative if you need access.)
- **AUTOGENERATE_INDEXES** - Instructs GPR to create indexes on all Datasets, Agent Profile schemas, and Customer Profile schemas. By default, set to `True`.

  > **Important**
  >
  > Genesys strongly recommends you to leave the default value for this variable.

- **HOST_DOMAIN** - Use this variable to specify the public IP address or host name used for your deployment. The value should be one of the following, depending on your environment type:
  - For single-server deployments, specify the public IP address or the host name of the host where GPR is deployed.

  - For high availability (HA) deployments, specify the IP address of your load balancer.
- **LOG_LEVEL**
  - **INFO** - Informational messages that highlight the progress of the application: **LOG_LEVEL**=INFO. This setting is recommended for production deployments.
  - **DEBUG** - Fine-grained informational events that are most useful to debug the application: **LOG_LEVEL**=DEBUG. This setting should be used only for short periods of time because it can fill the disk.
- **LOGIN_MESSAGES** enables you have the Predictive Routing application display a custom message on the login screen.
  - When you enter this message, make sure that all special characters are properly escaped. *Special characters* are ones not part of the standard English alphabet, such as symbols, letters with umlauts, cedillas, and other such marks, and letters from other alphabets, such as the Greek or Cyrillic alphabets.
  - To simplify the task of converting characters, Genesys recommends an online conversion tool, such as **https://www.freeformatter.com/html-escape.html**.
  - For example, make the following substitutions:
    - & becomes &
    - < becomes <
    - > becomes >
    - " becomes "
    - ' becomes '
- **OMP_NUM_THREADS** (required for releases prior to 9.0.011.00; in releases 9.0.011.00 and higher, this parameter is set automatically)
  - Genesys recommends that you set the value to OMP_NUM_THREADS=1 for the best performance.
  - If you do not specify a value, GPR spawns one thread for each core it detects in your environment. The system assumes it can use all available cores for tasks such as analysis and model training, leaving no CPU resources for other processes running on the same machine, such as reading/writing to the database. The result is an overall slowdown of the application. Set this variable to allow the operating system to properly distribute CPU threads among the various running processes.
- **S3_ENDPOINT** - (Mandatory) The endpoint for the Minio container, introduced in AICS release 9.0.013.01 for Dataset uploads and expanded to Agent and Customer Profile uploads in AICS 9.0.015.03. Specifies the public IP address or domain name of the server where AI Core Services is installed, followed, optionally, by the port number.
  - The port number must always be 9000, which is the mandatory port value allocated for the Minio container.
  - In HA environments, locate the server on which the Minio container is running and use the public IP address or the domain name of that server. For example:
    For an IP address - `S3_ENDPOINT=https://<public_ip_address>:9000`

    For a domain name - `S3_ENDPOINT=https://<your_domain_name>:9000`
  - The S3_ENDPOINT value must always use the HTTPS protocol. If you do not configure this variable, the **start.sh** script generates a warning message and stops deploying AICS.
- (Optional) **GUNICORN_TIMEOUT**

- Adjust the timeout if you need to accommodate a large Dataset. The current default value is `600` seconds.

## Configure AICS to Use HTTPS

The procedures here are those required to use HTTPS for connections among GPR components. HTTPS configuration for other components in your Genesys environment is covered in the *Genesys Security Deployment Guide* and in the product-specific documentation.

AICS supports HTTPS by default. Before you start using AICS, your organization should provide the certificates appropriate for your environment to enable the HTTPS connection protocol to work correctly. Genesys does not specify which certificates you should use.

After you have obtained the certificates, your procedure depends on your architecture:

- In a single-server environment, follow the procedure below.
- In a high availability (HA) environment, follow the instructions provided in the documentation for your load balancer. In an HA environment, you do not need to deploy the certificates on the individual nodes.

### Single-Server Environment

1. Copy the certificates to the ***<GPR_IP_version>*/conf** folder.
2. Rename the default certificates originally located in that folder using the following commands:
   ```
   $ mv tango.crt tango.crt_orig

   $ mv public.crt public.crt_orig

   $ mv tango.key tango.key_orig

   $ mv private.key private.key_orig
   ```
3. Rename the new certificates using the following commands:
   ```
   $ cp cert.pem tango.crt

   $ cp cert.pem public.crt

   $ cp priv_key.pem tango.key

   $ cp priv_key.pem private.key
   ```
4. Open the **tango.env** file and change the value for the **S3_ENDPOINT** variable from the IP address to the DNS name.
   For example, replace **S3_ENDPOINT**=`https://18.217.189.106:9000` to **S3_ENDPOINT**=`https://fce-u0009.us.int.genesyslab.com:9000`
5. Restart AI Core Services.

> **Important**

- When you use the GPR web application, check that the URL starts with `https://`.

**Next Steps**

- Configure ASC to Use HTTPS - When you configure HTTPS for Agent State Connector, use the same certificate as for AICS
- Configure URS Strategy Subroutines/Composer Subroutines to Use HTTPS

## Unusual HTTP/S Deployment Scenarios

- Default local certificate - Genesys ships AICS with a default local certificate. You can use that local certificate to access the GPR web application for internal testing purposes. Note the following points when using the local certificate:
  - The browser displays a Not Secure connection warning.
  - You **cannot** use the default certificate to configure connections from Agent State Connector or the Subroutines components to AICS.
- Self-signed certificate - *For lab environments only* - You can use OpenSSL to generate a self-signed certificate. You can use this self-signed certificate to configure secure connection between AICS and the other GPR components, as explained in the instructions for configuring HTTPS for ASC and the URS Strategy Subroutines.
  1. Generate a self-signed certificate by executing a command following the format in the following example:

     ```
     $ openssl req -new -newkey rsa:4096 -days 365 -nodes -x509 -subj "/C=US/ST=US/
     L=US/O=IT/OU=IT Department/CN=<ip address of the server where GPR is deployed>"
     -keyout tango.key -out tango.crt
     ```

  2. Accept the invalid certificate warning that appears when you open the GPR web application.
  3. If Dataset uploads from the GPR web application fail, navigate to the GPR Minio container at **https://<path_to-minio>:9000** and accept the security warning about the invalid certificate. You can then perform your Dataset uploads.
- HTTP connections in test environments - In AICS release 9.0.015.04 and higher, you can optionally configure HTTP connections.

  > **Warning**
  > HTTP connections are supported only in test environments. Genesys strongly recommends using the default HTTPS configuration in production environments and in lab environments that contain sensitive data. Genesys is not responsible for any potential damage and/or data loss if the solution is implemented without the recommended security practices and protocols.

  To use HTTP connections, perform the following steps:

  1. Comment out the following lines in the **/scripts/docker-compose.yml** file:

```
#    - ../conf/tango.key:/data/ssl/tango.key

#    - ../conf/tango.crt:/data/ssl/tango.crt
```

2. Edit the port configuration in the **/scripts/docker-compose.yml** file, as follows:
   Change

   ```
   443:3031
   ```

   to

   ```
   80:3031
   ```

3. Save your changes.
4. Restart GPR by running the following command:

   ```
   $ bash scripts/restart.sh
   ```

## Clean Up Disk Space

Starting in release 9.0.013.01, GPR performs automatic cleanup processes which should maintain an adequate amount of free disk space. However, if you are running an earlier version of AICS, or are running 9.0.013.01 or higher and continue to encounter disk space problems, refer to the instructions in this section.

You might encounter performance issues if you do not clean up Docker data that is no longer required. The Docker `prune` command enables you to clean up your Docker environment. The Docker user documentation provides a detailed discussion of the `prune` command and how to use it to clean up images, containers, and volumes; see Prune unused Docker objects.

> **Important**
>
> The clean-up process does not affect normal GPR operation. It does not require downtime, there is no need to restart any component, and performance is unaffected.

### Clean-Up Procedure

Genesys recommends that you use the following commands to remove unnecessary Docker data:

```
docker container prune -f
docker volume prune -f
docker network prune -f
```

To schedule regular cleanup jobs, use the `crontab` functionality to execute the appropriate command on every server where GPR is installed. The following example schedules the cleanup job for every Saturday at 1:00 am:

```
echo "0 1 * * Sat (docker container prune -f; docker volume prune -f; docker network prune
-f)" ) | crontab -
```

In an HA environment, Genesys recommends that you perform the cleanup on each node in turn.

If you need to configure your logging settings to avoid unacceptable log file sizes, see the following information:

- The LOG_LEVEL environment variable
- Configure AICS Log Settings

## (Optional) Configuring AICS for Large Datasets

A "large" dataset is one that contains more than 1.5 million rows/250 columns. No more than 100 of the columns should contain high-cardinality values. Genesys recommends that you adjust your dataset to stay within these size limits.

### Reconfiguring the GUNICORN_TIMEOUT Parameter

To accommodate a large dataset, you might need to configure the `GUNICORN_TIMEOUT` environment variable, which is located in the **.../<installation_directory>/scripts/tango.env** configuration file. The current default value is `600` seconds.

### Correcting an 413 (Request Entity Too Large) NGINX Error

> **Important**
>
> The NGINX container was removed in release 9.0.015.03.

1. Open the **nginx.conf** file.
2. Increase the value for the `client_max_body_size` parameter to `3g`.
3. Restart NGINX by entering the following command:

```
$ docker restart nginx
```

## (Optional) Change the Default Port for AICS

> **Important**
>
> If you change default port for AICS you have to make sure that port is opened to anyone who needs to access AICS APIs or UI.

If you are using NGINX, you must also change the port in your NGINX configuration. This section explains how to change the port for the Predictive Routing (Tango) application only.

> **Important**
> The NGINX container was removed in release 9.0.015.03.

Stop the application by running the following command:

```
$ bash stop.sh
```

Edit the **scripts/docker-compose.yml** file:

1. Locate the **tango-no-nginx** label.
2. Replace the listening port number with the new port number.

For example, to replace the default port, 443, by port 9090., replace `ports: "443:3031"` with `ports: "9090:3031"`.

Start the application by running the following command:. Note that you start the application without NGINX (there is no `-n` flag).

```
$ bash start.sh
```

Use your browser to check that the application is running on the new port (`9090`).

## (Optional) Turn on SSL/ HTTPS on NGINX

> **Important**
> The NGINX container was removed in release 9.0.015.03.

To turn on SSL and HTTPS on NGINX, perform the following steps:

1. Stop the application using the following command:
   ```
   $ bash scripts/stop.sh
   ```
2. Create a certificate or add the certificate and key using a command in the following syntax:
   ```
   $ openssl req -newkey rsa:2048 -nodes -keyout server.key -x509 -days 365 -out
   server.crt openssl dhparam -dsaparam -out dhparams.pem 4096
   ```
3. Update the **docker-compose.yml** file using the following commands:
   ```
   nginx:
   image: nginx:1.11.9-alpine
   container_name: nginx
   restart: always
   ports:
      - 80:80
      - 443:443
   volumes:
      - ./nginx-ssl.conf:/etc/nginx/nginx.conf
   ```

```
    - ./server.crt:/etc/nginx/server.crt
    - ./server.key:/etc/nginx/server.key
    - ./dhparams.pem:/etc/nginx/dhparams.pem
```

4. Uncomment (remove the pound sign from) the entire second section of the **nginx.conf** file. This sections contains the SSL configuration.
5. To enable HTTPS on NGINX, replace the following line in the **nginx.conf** file:
   `proxy_set_header X-Forwarded-Proto $scheme;`
   with: `proxy_set_header X-Forwarded-Proto https;`
6. Restart AICS using the following command. This is required to make the changes take effect:
   `$ bash scripts/start.sh -n</source>`
7. Verify that you can access Predictive Routing via HTTPS by opening the following URL in your browser:
   `https://<SERVER_IP_ADDRESS>/`

## (Optional) View Container Disk Usage

AICS uses persistent storage for two containers: Tango and Mongo. This storage configuration is defined in the `docker-compose.yml` file. Depending on your environment and its demands, you might need to change its configuration.

Disk usage might vary depending of the size of the organization and the use, but as a general rule, use a dedicated mount point at least for the **Mongo** container, because it is the fastest-growing directory.

### Tango Container

- **Host directory: /opt/SP/jop/temp/Medallia**
- Container directory: **/data/medallia**
- Usage: Contains the outcome of the call based on a survey.

- **Host directory: /opt/SP/jop/temp/GIM**
- Container directory: **/data/gim**
- Usage: Genesys Info Mart interaction records: interactions in the contact center, name of the agent, and so on.

- **Host directory: /opt/SP/jop/temp/CRM**
- Container directory: **/data/crm**
- Usage: CRM contains caller and customer profile information, products they own, tenure, and so on.

### Mongo Container

- **Host directory: /datadir**
- Container directory: **/data/db**
- Usage: Stores MongoDB data.

For extra information on Docker volumes, see Using Docker Volumes

## (Optional) Back Up Your Data

Genesys recommends that you back up necessary data, especially MongoDB data.

- The Disk Usage section offers a general discussion of the directories. See the Mongo Container section in Disk Usage to determine which directories should be backed up (the **Host directory**, for example) .

> ### Important
> For extra information about MongoDB backups: Backing Up MongoDB.

## (Optional) Map a Local Volume to a Container

You can map local directories or files into any of the containers used by the application: tango, workers, mongo, minio, or nginx.

To create the mapping follow these steps:

1. Update the **IP_JOP_PRR_<version_number>_ENU_linux/scripts/docker-compose.yml** file.
2. Edit the corresponding service section by adding a new line on the volumes declaration.
3. to make your changes take effect, stop and then restart the application, using the flags that may apply for starting the application.
   For example, to mount an existing local directory named `/some_local_directory` into the tango container at `/custom_mount_point` configure the volume would as follows:

```
volumes:
  - /opt/SP/jop/temp/Medallia:/data/medallia
  - /opt/SP/jop/temp/GIM:/data/gim
  - /opt/SP/jop/temp/CRM:/data/crm
  - /some_local_directory:/custom_mount_point
```

> ### Important
> - In releases earler than 9.0.015.03, the tango container can be started with or without NGINX. NGINX support was removed in release 9.0.015.03. It has two declaration options in the **docker-compose.yml** file: `tango` and `tango_no_nginx`. You should update both to avoid confusion.
> - Additional information can be found at https://docs.docker.com/compose/compose-file/compose-file-v2/#volumes

## Install into an Existing AICS Deployment

It is easy to install a different version of AICS on your target server. You can use the steps here to install either a newer or an older version of AICS.

> **Important**
>
> There is downtime during this process but no data is lost. Executing this script only upgrades services and does not stop or upgrade MongoDB.

> **Important**
>
> Review the Upgrade Notes section of the Release Notes for all releases later than your starting release, including your target release. Follow any procedures specified for the interim releases, such as running scripts. If there is no Upgrade Notes section, or the section is empty, no additional steps are required for the associated release. The following AICS releases *do* require special upgrade procedures:
>
> - 9.0.007.00
> - 9.0.007.01
> - 9.0.007.03
> - 9.0.011.00
> - 9.0.013.01
> - 9.0.014.00
> - 9.0.014.02

To perform the upgrade:

1. If you have custom values for any environment variables, make a copy of the **tango.env** file before you start your upgrade. For more about the environment variables, see Set Values for Environment Variables, above.
2. Copy the **IP_JOptPlatform_<*version_number*>_ENU_dockerlinux.zip** file to the desired installation directory. Genesys recommends that you use the PR_USER home directory as destination for the AICS installation package.
3. Unzip the **IP_JOptPlatform_<*version_number*>_ENU_dockerlinux.zip** file, using the Linux `unzip` command, to access the **IP_JOP_PRR_<*version_number*>_ENU_linux.tar.gz** repository file.
4. To unpack the **IP_JOP_PRR_<*version_number*>_ENU_linux.tar.gz** repository file, execute the following command:

```
$ tar -xvzf IP_JOP_PRR_<version_number>_ENU_linux.tar.gz
```

After unpacking the new version of AICS in the PR_USER home directory, you will have multiple

different subdirectories named **IP_JOP_PRR_<*version_number*>_ENU_linux**. For example you might have two subdirectories:

- **IP_JOP_PRR_<*old_version_number*>_ENU_linux**
- **IP_JOP_PRR_<*new_version_number*>_ENU_linux**

1. Assuming you are installing *new_version* of the application and removing *old_version*, execute the following commands in the **IP_JOP_PRR_<*new_version_number*>_ENU_linux** directory:

   ```
   $ bash scripts/install.sh
   ```

   ```
   $ bash scripts/upgrade_gpr_services.sh
   ```

2. Configure any environment variables you require, using one of the following methods:
   - Paste the copy you made of your previous **tango.env** file over the new one.
   - To preserve any newly-added environment variables, open the new **tango.env** file and edit it.

Your updated version of AICS should now be ready for use.

## (Optional) Uninstall AICS

The procedure given in this section should be used only on single-server deployments.

> **Important**
>
> If you need to remove AICS from an HA environment, contact Genesys Customer Care for assistance.

To entirely remove AICS, enter the following commands:

1. `$ bash IP_JOP_PRR_xyz/scripts/stop.sh # stop GPR`
2. `$ rm -rf IP_JOP_PRR_xyz # delete GPR installation`
3. `$ sudo docker system prune -a --volumes`

   or if this fails

   ```
   $ sudo docker system prune -a
   ```

4. `$ sudo rm -rf /datadir/*`

AICS should now be entirely removed from your environment.