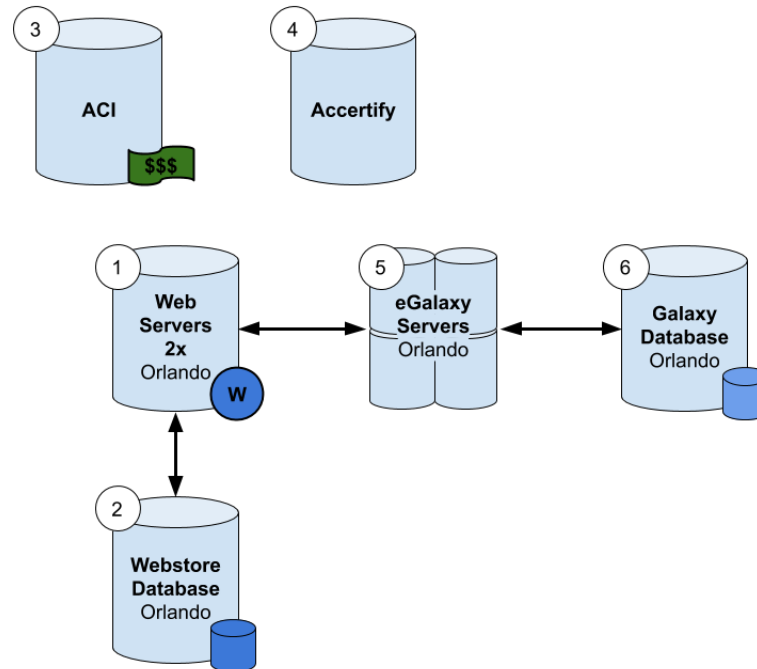


## Summary

The Agent Store platform is a fully-customized internal webstore which merges the Galaxy OLTS code base with a custom CMS tool. It is optimized with a checkout flow for Sales Agents in the Guest Contact Center (GCC).

## Network Topography Details



1. Internal traffic comes directly in to the web servers from the UNIV-CITY-FLA network via the load balancer at <https://usopagentstore.use.ucdp.net/> . This Load Balancer has two web servers behind it: uso16pasweb01 and uso16pasweb02. This application is used internally only and it is in the PCI zone.
2. When a user at the GCC picks up a guest call, the agent store knows nothing about the caller until the check out portion. However, the agent will enter their Promo Code/Login (usually OLTS+TMID)
3. Once a product is added to the cart a session is started, and database records are created. As the order progresses through the purchase process the database records are updated.
4. Integration to Avaya is mainly for Accertify purposes. Agent Store calls Avaya endpoint with the Agent's log in information (SSO). Avaya will return the guest's caller ID or an error message. If it returns a guest's phone number, the agent store will connect the guest's order number with guest's phone number.
  - a. Agent ID/Login
  - b. Order ID
5. When ready to checkout, the payment details are authenticated through ACI as payment processor via a connection to <https://lp-api-ist1.payments-portal.com:5443>

- a. Agent adds CC information on Agent Store. Agent Store sends raw CC information to ACI. ACI will send Agent Store back the tokenized CC if approved. Agent Store updates the Order Payment Line with the tokenized CC to process the transaction. Here's a sample if CC is declined:  
`<ACIResponse><ORD_ID>AS17483864</ORD_ID><aciAuthResponse.STAT_CD>DECLINE</aciAuthResponse.STAT_CD></ACIResponse>`
- b. New Proposed Flow for Payments:
  - i. Guest add CC information on phone keypad
  - ii. Intranext (capture tones)
  - iii. ACI approves or declines CC. If approved, tokenize CC
  - iv. Intranext (gets token, send to agent store over js)
  - v. agent store completes order using token through eGalaxy
6. Once payment is authorized, order is placed in a 100 status details are sent to Accertify and a fraud score is determined. The score will either:
  - a. result in the order to pass through or
  - b. be placed in a queue for manual review by Loss Prevention.
    - i. Loss Prevention team will either:
      1. Approve the order in Accertify which places the order in a 110 status. eGalaxy will pick up the order to finish processing it.
      2. Approve the order but order is blocked & add note in the Galaxy order note stating "this order is blocked by LP. Please contact the Command Center".
7. Once fraud check is completed, the application server marks the order as ready for import and a designated eGalaxy server connects to an eGalaxy handler to pick up the ready orders.
8. The eGalaxy process imports the order into the Galaxy database, where the order waits for the guest's visit to the park.

## Overview

## Server &amp; Environment Details

## Domain URLs:

- <https://uso08pwebpvip01.use.ucdp.net/AgentTicketStore.aspx> (Production)
- <https://uso08qawebpvip01.use.ucdp.net/AgentTicketStore.aspx> (QA)

## Production Web Servers (Orlando):

- USO12PWEBP20 (10.18.76.108)
- USO12PWEBP21 (10.18.76.109)

## QA Web Servers (Orlando)

- USO12QAWEBP20 (10.18.72.219)
- USO12QAWEBP21 (10.18.72.220)

## Databases (Orlando PCI)

- Production - USO08PDBGTS20 (10.48.10.179); Database – UniversalStudios
- QA - USO08QADBGTS20 (10.48.12.103); Database – UniversalStudios

## Access Control Information

The server environment and supporting databases are access controlled via Active Directory (AD) groups. This environment is hosted in the Orlando data center, and requires a UNIV-CITY-FLA domain account. Portions of this environment are behind the UNIV-CITY-FLA PCI firewall.

Note – User Management is required for this platform; Galaxy “Promotion Codes” are used for this purpose.

- **Domain Account** – A standard UNIV-CITY-FLA domain account is required.
- **UNIV-CITY-FLA PCI** – UNIV-CITY-FLA domain accounts must be granted access to the PCI firewall and PCI Authentication Tool by IT Security.
- **Server / Database Access** – IT Security manages access to AD Groups. Access is managed by being added to the “UITAdmissionsWebTicketConfig” AD Group in the UNIV-CITY-FLA domain.