

Appendix X – NY.gov ID Specifications
New York State Law Enforcement Records Management System



NY.gov ID Specifications

Introduction

The NY.gov ID Service provides a centralized user identity and access management solution for NYS Internet and NYeNET Intranet applications. It includes authentication and authorization services for secure websites, delegated administration services, and a self-care framework to allow for integration into application enrollment. This solution features a single sign-on capability across all NYS domains and provides NYS government users, business partners, and private citizens with a portal view with links to all applications to which they are authorized.

At the core of this solution is a secure directory of user profiles and application entitlements. User profile information is used to authenticate a user's identity at sign-on time. Application entitlements determine which applications a user is authorized to access. A set of administrative policies and procedures is used to establish consistency among the administrators from each program area who are responsible for managing their portion of this directory. NYSDS also provides delegated administration tools that allow application owners to control access to their resources, participating organizations to control their owned user accounts, and self-service functionality allowing users to maintain their own contact information. Complete password services are also provided.

Current NY.gov ID Usage

NYS uses this service for the following purposes:

- Storage of user authentication and authorization information for Single Sign on to NYS Web-Based applications.
- Resource for developers to leverage to build applications rich in dynamic content
- Single authoritative source for user credentials and other information
- Policy store for CA SiteMinder

NYSDS Components

The following table summarizes the software and platforms that comprise the NYSDS and associated services:

Software Package	Vendor	Version	HW Platform	OS Version
Oracle/Directory Server Enterprise Edition	Oracle	11.1.1.7.0	x86_64 / VMware ESX	RHEL 6
CA SiteMinder Policy Server/Web Access Manager CA SiteMinder Web Agent/Web Access Manager Agent	CA	r12.51 cr-01 r12.51 cr-01	x86_64 / VMware ESX (policy server) IIS, Apache, IBM HTTP Server (customer agents)	RHEL 6 Windows/Unix /Linux
Oracle Directory Proxy Server (DPS)	Oracle	11.1.1.7.0	x86_64 / VMware ESX	RHEL 6
NYSDS Delegated Admin. Software	In-House Application	2.1	IBM P-series	AIX 6
Login, Account Mgmt, Self Service, DAWS	IBM WebSphere	8	IBM P-series	AIX 6
Oracle 11gr2 Enterprise Edition Database Server	Oracle	11.2.0.4	IBM P-series	AIX 6

PingFederate	Ping Identity	7.1	x86_64 / VMware ESX	RHEL 6
--------------	---------------	-----	---------------------	--------

NY.gov ID Specifications and Details

The directory has a root suffix of “o=ny, c=us and contains branches for NYS Agencies, Local Government organizations, private citizens and business partners, both for profit and non-profit. Each branch in the Central Directory contains an ou=People and ou=Groups branch, however LDAP dynamic groups are heavily used as opposed to static groups for application access control. Each person entry in the directory is built with the following standard Object Classes:

- top
- person
- organizationalPerson
- inetorgPerson

The required and allowed attributes for each of these standard object classes can be found in the Internet Engineering Task Force (IETF) standard LDAP schema.

Additionally, ITS has extended the top object class to create additional objectclasses that are present in select user’s entries. Typical custom object classes include

- Nyperson - contains additional NYS specific user information (i.e. AgencyID)
- NYeNET-applications groups - contains application specific attributes used for access control and the basis for dynamic groups
- Nyacctllevel1 - contains account level attributes used for trust level of account

CA SiteMinder Usage and Details

- NY.gov ID uses CA SiteMinder to provide Single Sign On for NYS internal and citizen facing applications.
- NYS agencies utilize the CA SiteMinder web and application server agents to make their applications LDAP enabled. This makes their NYS applications capable of participating in this statewide SSO infrastructure.
- CA SiteMinder is currently supporting password-based authentication for all applications requiring this service.
- CA SiteMinder is deployed in a fully redundant manner to provide 7/24/365 service.

Oracle Directory Proxy Server (DPS) Usage and Details

- Provides for failover and load balancing of directory resources
- Allows NYS users LDAP lookup capability for application information

NY.gov ID Delegated Admin Software Usage and Details

- Allows NY.gov ID Admins to create, delete, and modify NY.gov ID user accounts
- Allows NY.gov ID Admins to create, delete, and modify NY.gov ID entitlement. and other application-specific attributes

NY.gov ID Delegated Admin Web Service (DAWS) Software Usage and Details

- Allows NY.gov ID Admins to create, delete, and modify NY.gov ID user accounts
- Allows NY.gov ID Admins to create, delete, and modify NY.gov ID entitlement. and other application-specific attributes

Appendix X – NY.gov ID Specifications

New York State Law Enforcement Records Management System

Account Management Services Usage and Details

- Allows NY.GOV ID users to change their password.
- Allows NY.GOV ID users to change and set their shared secrets.
- Allows NY.GOV ID users to view their application entitlements.
- Allows NY.GOV ID users access to maintain their contact information.

Oracle Database Servers Usage and Details

- Functions as the repository for the CA SiteMinder Audit logs

NY.GOV ID Federation Service

- NY.GOV ID uses PingFederate from Ping Identity to provide Federation Services.
- NY.GOV ID can generate SAML assertions with user's NY.GOV ID identity and can consume SAML assertions generated by external identity providers and provide SSO to NY.GOV ID SSO environment.
- NY.gov ID Federations service supports SAML 2.0 and WS-Federation per SAML OASIS standards.

Additional Information

- Schema checking is enabled in the NY.GOV ID
- UID's are unique across the entire NY.GOV ID
- The NY.GOV ID is replicated and load balanced across multiple servers
- NY.GOV ID has not modified any standard LDAP objectclass or misused any standard attributes
- The NY.GOV ID utilizes Delegated Administration as well as bulk loads to populate and maintain the directory entries
- NY.GOV ID will work with the successful bidder in making schema changes as needed for applications use of the ny.gov ID directory.
- Access to the NY.GOV ID is strictly controlled by a combination of Directory ACL's, Oracle DPS, and Firewalls.