

NYS Directory Services – Service Detail

0220.00

0221.00

0222.00

0223.00

Overview:

NYSDDS is a centralized user identity and access management service for Statewide Internet and intranet applications. The NYSDDS solution includes a single sign-on capability across all domains and can provide state and local government, business partner and private citizen users with a personalized view of all applications for which they have been authorized. The service currently protects over 120 web based applications owned by numerous state agencies. The total end user base is 850,000 and counting.

NYSDDS features include:

- ▶ Centralized user identify and access management
- ▶ Single sign on capability
- ▶ Flexible access and authorization solutions
- ▶ Delegated Administration
- ▶ Self Registration Services
- ▶ Self Administration Services
- ▶ Forgotten Password Services
- ▶ Consulting services
- ▶ High availability
- ▶ 24X7X365 support

Security:

At the core of NYSDDS is a secure directory of user profiles and application entitlements. Applications leverage information contained within the directory for authentication, authorization, building dynamic content, and sharing information across state and local government entities.

User profile information is used to authenticate a user's identity at sign-on time. This is known as Authentication. Additionally, application entitlements determine which applications a user is authorized to access. This is referred to as authorization. Finally, a set of administrative procedures are used to establish consistency among the administrators from each program area who are responsible for managing their portion of the directory. The combination of authentication, authorization and administrative procedures allows you the ability to create the security solution you need to best protect your application.



Features:

Delegated Administration (DA) Tool:

NYSDS provide you the ability to manage the identities and access abilities of your end user population via the web. This is achieved by using a ITS application named the Delegated Administration Tool.

Delegated Administration (DA) is a web based software application that provides the ability for administrative users, (also known as Delegated Administrators), to manage his or her agencies' end user accounts in the directory. Authentication of an end user account is controlled by the Delegated Administrator and the administrative abilities are:

- ▶ Create
- ▶ Update
- ▶ Disable
- ▶ Enable
- ▶ Remove
- ▶ Reclaim
- ▶ Reset Password
- ▶ Report generation

Authorization is enable on an end user profile when attributes are added to the end user account. Application owners or entitlement administrators can change these attributes on the end user account via Delegated Administration (DS) Tool, to grant or deny access to applications as needed.

Consulting Services:

NYSDS employs technical experts that will assist you through the creation and implementation of an appropriate security solution for your application.

High Availability:

Downtime is minimal now that the NYSDS producti8on environment is comprised of two physically and geographically separate Data Centers. Each production Data Center is an exact replica of the other with respect to software and hardware. Data Integrity is maintained across sites via real-time replication. In addition, all NYSDS production is monitored 7X24X365 by Data Center Enterprise System Monitoring, providing you around the clock support.

Self-Care:

NYS DS provides the ability for your end user population to manage some aspects of her or his user account. By taking advantage of the Self Care utilities your agency will reduce the resources spent on managing user accounts. The Self Care consists of three utilities: Self Registration, Self Administration and Forgotten Password Services (FPS).

- ▶ Self Registration is a web application that allows any person to register for a NYSDS account. It can be configured to collect application specific information on a per-application basis if desired.
- ▶ Self Administration is a web based application that is available to all registered NYSDS users. It allows users to update most personal and application specific attributes associated with their account.
- ▶ Forgotten Password Services allows users to reset their own passwords.

Benefits:

By using NYS Directory Services for application security, participating organizations can free up internal resources. Maintaining data in a single properly architected identity management solution, such as the directory, coupled with defined policies and auditable procedures also enhances compliance with privacy and confidentiality laws and directives.

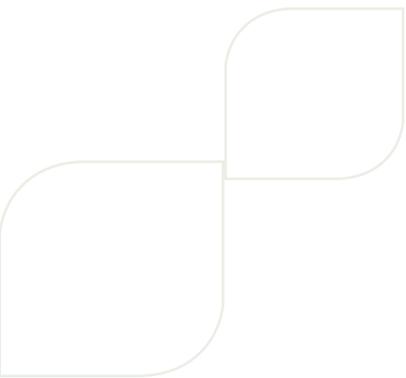
How an Organization Participates in the NYS Directory Service (NYSDS):

For an organization to become a Participating Organization (PO) of the NYSDS, both administrative and technical tasks need to be accomplished.

Administrative signup tasks:

Performer: Organization requesting participation in the NYSDS. The person(s) performing this procedure should have the authority to give or obtain the necessary executive approvals for participation.

- ▶ Contact the ITS Customer Relations Team, using the contact information provided at the end of this document, to set up an initial requirements meeting with the appropriate ITS staff.
- ▶ Obtain and read the NYS Directory Services – Directory Account Management Policy*. [See <http://www.cio.ny.gov/Policy/index.htm> under Risk Management, G07-001 entitled “Best Practice Guideline on Identity and Access Management: Trust Model”]
- ▶ Select the primary contact (PO DSA) for your organization.
- ▶ Suggested Guideline – Consider the PO’s Information Security Officer or the Human Resources Director for the PO DSA role. At a minimum, involve them





in deciding who the appropriate person in your organization is for the role. The PO DSA does not need to be a technical person in the organization.

- ▶ The organization's ISO (or in lieu of an ISO, the person in the organization with roles & responsibilities similar to a security officer) will submit a completed NYSDS Participation Request Form to the NYSDS group.
- ▶ Receive notification from the NYSDS group that a PO DSA account has been established in both the development and production environments.
- ▶ Return Completed Forms to ITS Customer Relations via email: customer.relations@cio.ny.gov or Fax: 1-518-474-1196. For additional questions contact Customer relations at: 1-866-789-4OFT(4638).

How to Request a Security Solution for Your Organization's Web based Application:

- ▶ First, to deploy an application using NYS Directory Services your organization must already be a participating organization, see above.
- ▶ Complete the Application Registration Form to establish Application Owner NYSDS Application Registration Form The participating organization's ISO will identify the person who will be their single point of contact to ITS regarding the integration of the application and the recommended security solution. Once the application is deployed and protected the Application Owner becomes the person responsible for approving entitlement ability for and accessibility to the application. This form must be signed by ISO or person acting in similar position. It must also accompany the Application Questionnaire.
- ▶ Complete the Application Questionnaire NYSDS Application Questionnaire This form provides technical information regarding your application. We use this information to determine the security solution that will meet your needs.
- ▶ A completed NYSDS Application Questionnaire and Application Registration form must be submitted for each application that the participating organization wishes to deploy.

Return Completed Forms to ITS Customer Relations via email: customer.relations@cio.ny.gov or Fax: 1-518-474-1196. For additional questions contact Customer relations at: 1-866-789-4OFT(4638).



Frequently Asked Questions:

Question: What information will the directory contain?

Answer: Primarily, the NYSDS directory will contain entries for state and local government employees, business partners and citizens who need access to NYSDS protected applications. Each person's entry will minimally contain name, e-mail address, userid, password, and shared secret information.

Question: How will the directory be administered?

Answer: NYSDS utilizes a concept of delegated administration, allowing account administration of the directory to be securely administered by people in the best position of knowing the actual content. For example, specifically identified administration within an organization can be given the ability to create, update, and remove accounts, while application owners (and delegates) can be given the ability to grant/revoke access to applications. Furthermore, self-administration lets users update their own contact information.

Question: Does the NYSDS support multi-factor authentication?

Answer: The NYSDS infrastructure is capable of supporting multi-factor authentication.

Question: Will the NYSDS provide a network authentication service?

Answer: ITS has developed the New York State-Wide Enterprise Directory (NYSWED), a Microsoft Active Directory infrastructure, for this purpose. Please consult with your ITS Customer Relations Manager for more details.

Question: Does NYSDS provide single sign-on?

Answer: Yes. Single sign-on can be provided to all web applications utilizing NYSDS security.

Question: What is the structure of the directory?

Answer: The basic structure of the underlying NYSDS directory follows the organizational characteristics of state and local governments. This allows for secure delegated administration and efficient use of Access Control Lists (ACLs) for security.

Additional Information:

Cost

Please contact ITS Customer Relations at customer.relations@cio.ny.gov or 1-866-789-4638 or see our website at www.cio.ny.gov for additional information.