THE CLIENT

A large city government, bigger than many state governments, that has multiple and differing organizations under its control—from library services, law enforcement and public utilities to telecommunications infrastructure, transportation departments and recreational facilities.

Individual departments and organizations all have specialized systems that need local administration and customized access, yet all the departments must have a common way to communicate employee status and general access rights across the entire government.

1 THE CHALLENGE

The government implemented an identity management solution to provide a common framework across multiple departments. However, the specialized administrative and access needs for individuals in different departments varied so widely that creating specific roles became too time-consuming, complex and costly to manage.

TIME-CONSUMING

- Centralized IT spent more time creating and managing roles than granting timely access.
- Centralized IT received too many requests for specialized access and administration to manage.

COMPLEX

- Workers in each department needed access and administration rights to department-specific applications.
- Access and administration needs changed in frequent, subtle ways.

COSTLY

- Creation of appropriate roles often meant extra hours or bringing in experts.
- Fine-grained delegation of administrative rights in the identity management solution required extensive customization.

2 THE NETIQ SOLUTION

By using NetIQ® Directory and Resource Administrator™, the government delegates administration of local Active Directory domains to individual departments and lets agencies manage needed administrative rights. The identity management solution continues to manage the larger identity lifecycle of each employee and to provision access to key critical systems and resources.

DELEGATED ACTIVE DIRECTORY ADMINISTRATION

- Local admins have the ability to selectively administer target groups and organizational units.
- Those closest to a problem can respond to most access needs without central IT having to create and manage an ever-changing catalog of roles.
- Central IT can manage key systems and overall identity while easily allowing individual departments to delegate local administration.

3 THE RESULT

By implementing secure Active Directory administration, the government reduced the workload on the centralized IT department. The implementation granted more specific, localized and timely access to systems and reduced the costs of creating and managing department-specific roles, all without compromising the overall identity and security framework.

REDUCED WORKLOAD

- Centralized IT is not consumed with creation and management of department-specific roles.
- Department admins can specifically manage what they need without asking centralized IT for access.

TIMELY ACCESS

- More people get access to local, departmental systems quickly.
- Most administration happens at a local level.

REDUCED COSTS

- Less need for outside experts to create roles.
- Centralized IT provisions access to key, critical systems and resources.
- Local admins respond more quickly to minor issues.

4 PRODUCT/SERVICE IMPLEMENTED

NetIQ® Directory and Resource Administrator™

UC40002DRAL PO 04/13 F