ONE IDENTITY by Quest

City gets Active Directory right, securing citizen and employee information

Active Roles removes cumbersome and error-prone manual processes from Active Directory user lifecycle management

THE CITY OF COPPELL

Country: **U.S. Texas**

Population: **Just under 50,000**

Industry: **Local government**

Website: **www.coppelltx.gov**

The challenges of identity and access management (IAM) – namely ensuring that the right people, have the right access, to the rights systems, in all the ways they want, and that those in charge can verify the "rightness" of that access – is difficult in most organizations, but even more so in local governments. With a wide mix of user types ranging from employees to contractors and from citizens to vendors, it becomes very difficult to get it right. The city of Coppell, Texas is no different from most municipalities, but Coppell was able to get much of IAM right.

"The City of Coppell is a first-rung city relative to Dallas," said Jerod Anderson, assistant chief information officer for the city. "We cover about 14 square miles and have a population just under 50,000. With all the recent breaches, it is becoming more critical than ever that we secure our users' information and data whatever type of user they may be. We see a lot of exposure out there in the news, and we at the city don't want to be one of them – we're looking for tools to help us prevent that exposure."

Challenges

- **To minimize risk and exposure**, while securing users' critical information and data
- **Easy provisioning and deprovisioning** with a wide mix of user types, including citizens
- **Developing a role-based security model**

Results

- **Reduced IT staff workload**
- **The ability to build custom policies** and custom workflows that gives access across all applications
- **Facility to grant each administrator only the permissions necessary** to do the job
- **Easy to deploy and use**

Solutions

- **Active Roles**

> **Active Roles allows us to build customizable workflows that enabled us to create a single portal and one set of AD data that gives access across all of our applications.**
>
> *Jerod Anderson, Assistant Chief Information Officer, City of Coppell*

As with any other government entity, the City of Coppell manages a high volume of citizens' personal information. This information runs the gamut from social security numbers and credit card information to court records and medical information. To add to the risk, the ways citizens and employees access this information has expanded to include a variety of cloud options, mobile phones, and traditional online access.

"As a city we have lots of contractors and vendors that need access to specific systems or data for a while, but not permanently," said Pallavi Kalamkar, systems administrator for the city. "My job is to build the security model around our enterprise applications. Securing data when it comes to third-party access is critical. Our goal is to implement a role-based security model. So if someone in one department needs access to certain sets of data or capabilities of an application to do their job, we grant them the access they need but not unlimited access to every piece of data or the full range of application functionality. The same principle applies to temporary access – we want to grant it only for as long as it's needed."

A major component of the city's enterprise is Microsoft Active Directory (AD). Every user has an AD account and a majority of access transactions are conducted via AD. Key to successful administration of access when AD is involved is accurate, thorough, and quick provisioning and deprovisioning of user accounts. "As we provision and deprovision people we need to be consistent in terms of what functions are appropriate for that particular user," said Kalamkar.

"So for example a person with the role of Payroll Analyst should have access to certain systems and certain parts of systems. We do that by putting them in groups mapped back to the role – but with the native tools that come with AD, it could take up to two days to complete the process."

"We did not have the ability to standardize on what a role was," added Anderson. "And with our goal to have a role-based security model, the inability to assign people to a specific role that will then, automatically, provision them correctly into Active Directory was a big problem that was preventing us from achieving our security objectives. Historically it would take days or even weeks to get someone completely and correctly provisioned, and often it didn't happen until someone called to tell us what access was missing."

To overcome this challenge and enable the role-based security model the city was after, Anderson and Kalamkar selected a solution called Active Roles from One Identity. Active Roles is a management and security tool optimized to address the needs of Active Directory and AD-connected systems.

> **Every department can now take ownership of things like creating a new employee and setting up all the correct access. All thanks to the customized workflows and dynamic groups available through Active Roles.**
>
> *Pallavi Kalamkar,*
> *Systems Administrator, City of Coppell*

"One of the key benefits of Active Roles is the reduction in workload on the IT staff," said Anderson. "It allows us to build customizable workflows that enabled us to create a single portal and one set of AD data that gives access across all of our applications."

"Now that we are able to build custom policies and custom workflows, it has made our lives in IT easier," said Kalamkar. "Now we can add a user to a specific group, provision their home folder and the license assignments in one automated step thanks to Active Roles. Where this used to be entirely the responsibility of IT, now we can decentralize and place the power in the hands of the right people. So every department can take ownership of things like creating a new employee and setting up all the correct access. All thanks to the customized workflows and dynamic groups available through Active Roles."

In addition to the user lifecycle management, or provisioning, benefits Active Roles delivers to the city, it also brings the added benefit of creating a security "firewall" around AD. Natively the Active

Directory Admin account is an all-or-nothing, universal credential that presents a high level of risk due to its power and the number of people that, by necessity, share the account. With Active Roles, the city is able to implement role-based security on the AD Admin account as well, granting each administrator only the permissions necessary to do the job – nothing more, nothing less.

"The ability to assign someone in a department the permissions to set up a new user, without granting them full AD Admin permissions is huge," said Anderson.

> **Without Active Roles, that would be impossible.**

"Active Roles was easy to deploy," continued Kalamkar. "The time savings, cost savings, automation, and integration make it easy for me to recommend." "If I was talking with a colleague and was asked to recommend a tool to help them address some of their access management needs, I would definitely tell them about One Identity and Active Roles," added Anderson. "You can take it to where you need it to go and a lot of it is straight out of the box. Active Roles is a really wonderful tool.

About One Identity

One Identity delivers unified identity security solutions that help customers strengthen their overall cybersecurity posture and protect the people, applications and data essential to business. Our Unified Identity Security Platform brings together best-in-class Identity Governance and Administration (IGA), Access Management (AM), Privileged Access Management (PAM) and Active Directory Management (AD Mgmt) capabilities to enable organizations to shift from a fragmented to a holistic approach to identity security. One Identity is trusted and proven on a global scale – managing more than 500 million identities for more than 11,000 organizations worldwide.

For more information, visit www.oneidentity.com.

ONE IDENTITY by Quest