CASE STUDY

University streamlines administration and enhances security with a unified approach to IAM

One Identity solutions empower Canadian University Dubai to streamline identity administration and governance processes from 48 hours to 5 minutes

Key Facts

Company
Canadian University Dubai

Industry
Higher Education

Country
United Arab Emirates

Employees
4,000 students, 400 faculty and staff

Website
www.cud.ac.ae/

Challenges

- Risk associated with highly mobile, and constantly evolving user population
- IT-intensive administrative processes delayed user and student achievement
- Establishing a proactive security stance

Results

- Overcame role creep and established a unified approach to permissions and access management
- Reduced provisioning time from 48 hours to 5 minutes
- Empowered students to manage access remotely and in the manner they prefer without sacrificing security
- Facilitate rapid adoption of new technologies and a move to the cloud

Product

One Identity Manager

One of the biggest challenges facing institutions of higher education is the cyclical nature of access controls. At the beginning of every semester, high numbers of students suddenly need appropriate access to university systems, faculty and staff permissions must be adjusted, and IT's workload shifts from routine maintenance to critical remediation overnight. Such was the case with Canadian University Dubai (CUD).

Located in the United Arab Emirates, CUD is a private institution that provides a Canadian curriculum-based education for more than 4,000 students representing more than 100 nationalities. Its faculty and staff is made up largely of expats from North America and Europe.

"One of the things I love about the University is the fact that as a private institution, I'm able to always work with the latest technology and the

ONE IDENTITY

> ""One Identity Manager provides the tools we need to control and manage all of the roles and security permissions we have to deal with. **Its level of flexibility and governance** across our very diverse identity landscape is ideal for us.""
>
> *Mohammad Fayaz, IT Applications Manager at Canadian University Dubai*

most modern applications," said Mohammad Fayaz, IT Applications Manager at CUD. "It allows me to evolve technologically and keep my career up to date as well at take the University to the highest standard possible. But that technological sophistication also has its challenges both from an operational and security standpoint."

Fayaz is focused on protecting student data as well as CUD's brand identity. "Security is more critical than ever," he continued, "every day companies are getting hacked. Data is the new wealth. Our students and their parents rely on us to protect their data. One of my biggest areas of focus is ensuring that that data is secure from internal and external threats. Identity and access management (IAM) is on the front lines of that battle."

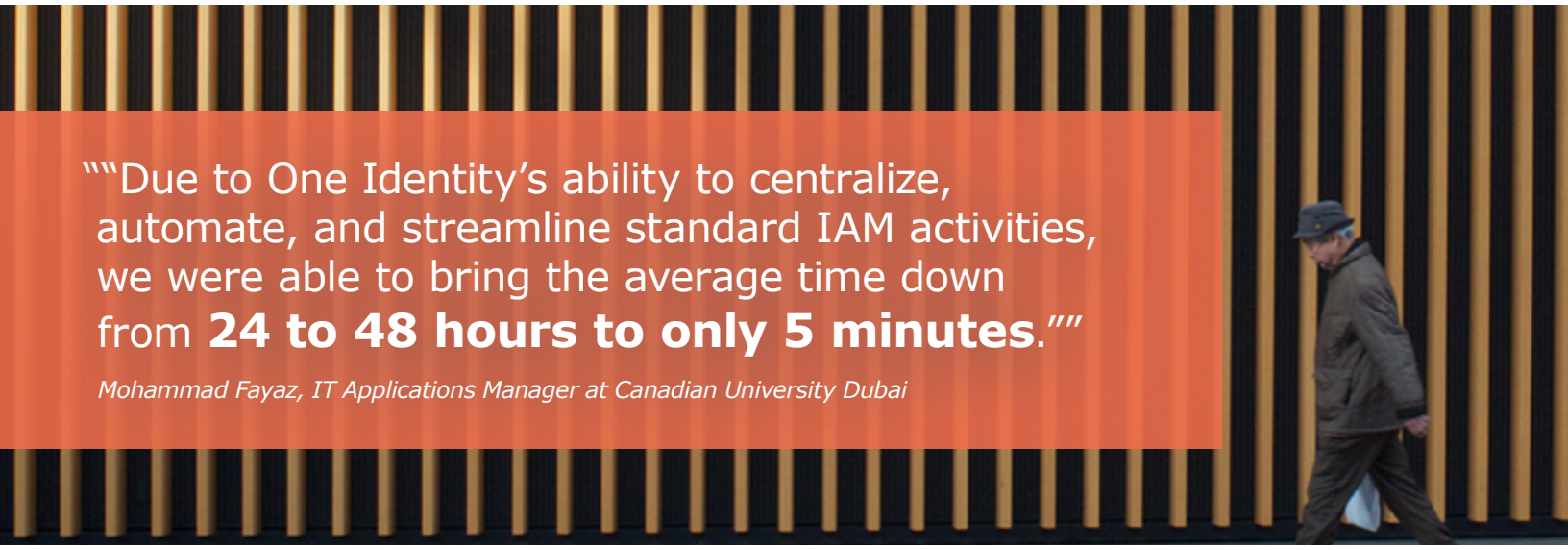
CUD's biggest IAM challenge is the management of security roles and the provisioning of accounts across a very wide range of systems. Each new system or application that is added to the enterprise introduces another layer of security that must be managed by Fayaz and his team.

"It was a big hurdle for us to provision accounts," said Fayaz. "It was so time-consuming to provision all of the accounts into all the different systems we have, and then track them to ensure that there is no role creep. We need to set up the access for users so they can get to the right resources but we need to make sure that they have only the rights they need with no added privileges, roles, or permissions assigned to them, which introduce unacceptable risk."

The legacy process for managing user access at CUD demanded high amounts of IT intervention. As a need for access was identified the IT department would have to gather the requests; login individually to each affected system; set up the user accounts and assign permissions, roles, and responsibilities; and then provide the necessary login credentials to the user. "Obviously this was a very time-consuming process," added Fayaz.

"As a mid-sized organization, the roles and responsibilities we manage change from time-to-time," said Fayaz. "And that doesn't even take into account the seasonal influx of provisioning activities demanded at the beginning of every semester. Managing provisioning and permissions often took 24 to 48 hours – for each user. Obviously there were manual errors and miscommunication between the requester and the IT department. That's a lot of risk."

In addition to the inefficiency of manual provisioning processes, CUD found that often users were mistakenly provided with extra access permissions that they did not need. With the best intentions, a manager would approve provisioning actions but lacked the enterprise visibility to discover unforeseen risk. CUD had a two-headed monster of IAM danger – extreme inefficiency due to a complex enterprise and a reliance on manual processes, and lack of visibility (or governance) into the consequences of those provisioning actions.



> ""Due to One Identity's ability to centralize, automate, and streamline standard IAM activities, we were able to bring the average time down from **24 to 48 hours to only 5 minutes**.""
>
> *Mohammad Fayaz, IT Applications Manager at Canadian University Dubai*

"We needed a way to bring automation, consistency, and oversight to our provisioning and access management practice," said Fayaz.

The University turned to One Identity to help address its classic IAM challenges. CUD selected One Identity Manager, a powerful enterprise provisioning governance solution, and One Identity Password Manager, a password management solution that includes granular password policy and a full-range of secure self-service password management capabilities.

"Thanks to the One Identity solutions, we were able to overcome the huge IT bottlenecks that we traditionally experienced at the beginning of each school year," said Fayaz. "One Identity dramatically improved our turnaround times for provisioning accounts and password resets. Due to One Identity's ability to centralize, automate, and streamline standard IAM activities, we were able to bring the average time down from 24 to 48 hours to only 5 minutes."

Fayaz reports that One Identity Manager was able to embrace the granular nature of access needs throughout the University. With both undergraduate and graduate students across multiple disciplines and varying levels of faculty along with multiple tiers of administrative staff and officers, One Identity Manager's ability to centrally define each role, provision the correct access for each across the entire enterprise, and deliver the visibility necessary to perform the mandatory governance activities of certifying the appropriateness of that access provided the end-to-end IAM visibility and control the University previously lacked.

"One Identity Manager provides the tools we need to control and manage all of the roles and security permissions we have to deal with," said Fayaz. "Its level of flexibility and governance across our very diverse identity landscape is ideal for us."

In addition to provisioning and governance, CUD also turned to One Identity for help with its password issuance and management challenges.

"Prior to partnering with One Identity, every user started out with default passwords and it was their responsibility to come to the IT department to change it that typically took more than 24 hours – a risky and inefficient process," said Fayaz. "Now, they are able to actually change the password from their office or remotely on their mobile phone in about 5 minutes. With one click they are able to access the portal, they receive a temporary security code via SMS and after verifying their identity they can easily create a new password – Password Manager makes sure it adheres to our security policy, and IT doesn't have to get involved at all. It even reminds them when it's time to reset their password, which was impossible before."

"When it comes to security, your reputation is on the line, you don't want to be the next hack headline" continued Fayaz. "One Identity provided us with the tools to manage our most troublesome IAM areas. One Identity is very technically sound, very responsive, and have the vision and strategy to support our long-term plans. As we move more to the cloud and continue to innovate, One Identity's ability to evolve with us through additional automation, integration, scope, and flexibility is going to be key to our success."

Learn more at OneIdentity.com

ONE IDENTITY