



Mindtree

A Larsen & Toubro Group Company



Securing
applications on
Azure using
identity and
management

A Mindtree White Paper / May 2021

Welcome to possible



Introduction

AIAM (Azure Identity and Access Management) is one of the services of Azure security and access control for managing one's user identity. The global admin of Azure account has the authority to find out which user has what type of access, and what actions can the user perform on that particular access by using IAM.

The aim of IAM is to identify, manage, and control the users by providing required access to the users.

Challenges

1. In the cloud environment there is a challenge of providing identity and access management for cloud and hybrid environments.
2. Another major problem is consumer IAM in the cloud environment. What if we want to join virtual machines in Azure to a domain without deploying domain controllers?
3. Other issues includes those of assigning licenses, provisioning identities to applications in Azure AD, troubleshooting, and remediate license assignment errors.

Solutions

1. It is easier to preserve access to the services with the help of Azure IAM solutions. Applications can be secured in the initial stages using Azure IAM solutions.
2. Provide protection from invalid login hits and secure credentials from uncertainty. One can make use of the identity protection tools, risk-based access controls and better authentication options to secure credentials without disturbing productivity.

Description

1. Assigning roles using the Azure portal:

Azure role-based access control is an authorized system which is used to manage access to the Azure resources. Here, roles are mainly the combination of multiple permissions.

In Azure RBAC, the user who wants to provide access to an Azure resource should have 'write' permission, should know who needs access and what type of access they need.

Generally, Roles can be assigned to service principal, users, managed identity, and groups. In the managed identity, the user who is trying to provide access needs to check for the user assigned managed identity and system assigned managed identity.

The user needs to find out the scope, which has different levels like resources, resource groups, subscription, and management groups, which is structured like a parent-child relationship.

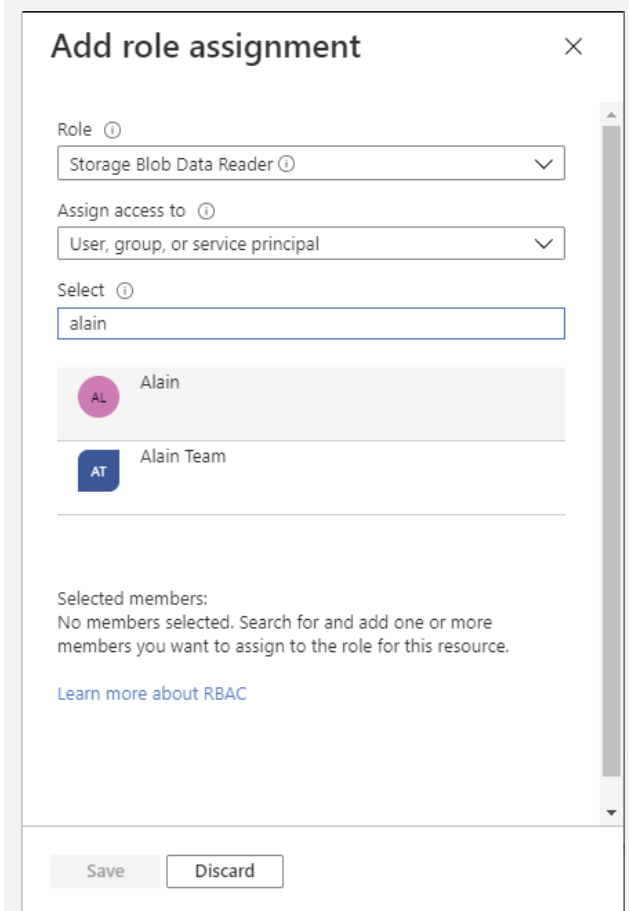
Roles can be assigned at different levels of the scope. The role will be applied according to the level of scope that has been selected. The child levels can inherit the roles assigned to the parent level. The roles which are assigned in managed groups can be applied to all the inherited levels like resource, subscription, and resource groups. Assigning the roles can be done not only in the portal but also through *Azure CLI, Azure PowerShell, and Rest APIs*.

Each subscription allows to have 2000 role assignments, including custom roles and built-in roles. Each level scope allows to have up to 500 roles.

It is better to avoid assigning roles at higher levels of scope to avoid risk for the resources

Assigning roles using the Azure portal:

1. Go into the **Azure portal** and search for the scope like specific **Resource or Resource groups or Subscriptions or Management groups**.
2. Open the **Access control/IAM**, to see the **role assignments** at that specific scope, click on Role Assignments tab.
3. To add any role assignments, click on **Add** option and select **Add role assignment**. User should have permission, otherwise further options will be disabled in **Add** section.
4. In the **Role** section, find out and select the role from the available roles.
5. In **Assign access to**, choose the type of **security principal** who needs access.
6. In **select** section, select the security principal like **username or group name**.
7. click **save** and the assigned will be displayed in the **role assignments** section.



Add role assignment

Role ⓘ
Storage Blob Data Reader ⓘ

Assign access to ⓘ
User, group, or service principal

Select ⓘ
alain

AL Alain

AT Alain Team

Selected members:
No members selected. Search for and add one or more members you want to assign to the role for this resource.
[Learn more about RBAC](#)

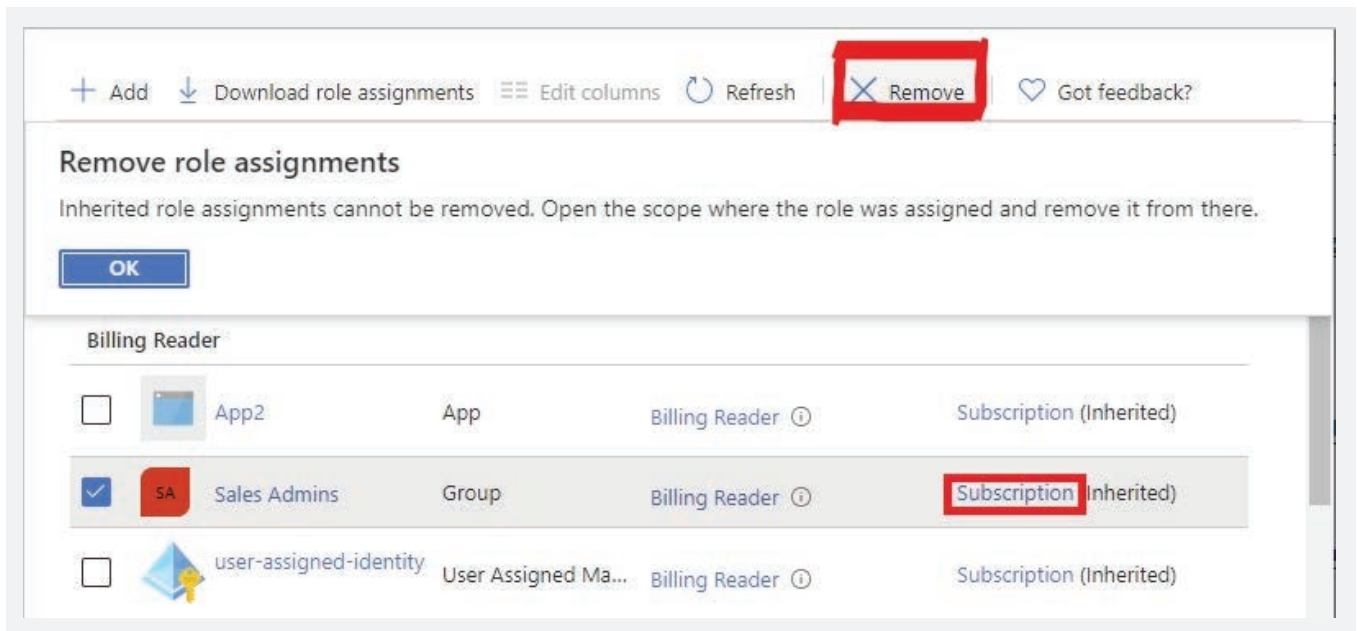
Save Discard

Steps to remove role assignments:

To remove access from an Azure resource in the Azure Role based access control, remove the role assignment. Follow the below steps to remove a role assignment.

1. Open **Access control/IAM**. Click on **Role Assignments** tab, the role assignments at that specific scope will be displayed.
2. Select the role assignment which must be removed and click on **Remove**. A dialogue box will appear showing **'remove role assignments'**, click on **yes**.

3. If the role assignment that is selected to remove is at child scope, which are inherited from the parent scope, it shows a message saying ***Inherited role assignments cannot be removed.*** Then at the scope, open **Access Control (IAM)** scope where the role has been assigned and try to remove or click on **subscription link** in the **role assignments** list.



2. Azure Active Directory

Azure active directory – it's a next version of the cloud-based *identity and access management solution (IAM)*, it helps organizations where the user have single login credentials to access all the services that are permitted by the administrator.

Who can use Azure active directory?

IT Admins: As business demands to use more resources and apps, there must be some control over the access to these apps and resources. Therefore, Azure active directory helps to control the access of these apps and resources.

Application developers: As a developer, one needs to use multiple apps or resources to build applications. The Azure active directory helps by providing a *single-sign-on (SSO)* to the applications. This helps the developers to complete the work quickly.

Online customers/subscribers: Some of the services like *Microsoft 365, office 365, Dynamic CRM and Azure*, already use the Azure active directory, hence these online customers become an Azure active directory tenant.

Azure Active directory licenses:

If we use any of the Microsoft online services, then we get Azure active directory with access to all the free features.

- 1) **Free:** In the free Azure active directory license, it provides some basic reports also. For the cloud users, it provides self-service password change, single sign-on option for SAAS apps, and also single-sign-on is assigned for 10 apps per user.

- 2) **Premium P1 license:** In P1 license, you get unlimited directory objects. Also, users can access both on-premises and cloud resources, for an on-premises users self-service password reset is allowed. This plan allows advance level administration like dynamic groups and advance report.
- 3) **Premium P2 license:** All the features available in P1 along with some extra offers, like -we can review the access. The P2 license has Azure active directory identity management, privileged identity protection, and privileged identity management help to monitor, restrict the administrators and also help to access their resources.
- 4) **Pay-as-you-go license:** Basically, this license supports the customer from the business-end. It has one feature called B2C, which means Azure active directory business-to-customer, where this feature is helpful for the customers when they face any issues or if they are using any apps.

The pay-as-you-go license helps IAM solution in order to support the customer from the business point.

Terminology of the Azure active directory:

- 1) **Azure active directory:** Azure active directory – it's a next version of cloud-based identity and access management solution (IAM), it helps organizations where users have single login credentials to access all the services that are permitted by the administrator.
- 2) **Identity:** Identity is nothing but validating the user, where the user has a set of credentials, which has username and password.
- 3) **Account:** Once we have the identities, we can use those identities to create accounts.
- 4) **Single tenant:** Single instance of software and its supporting infrastructure, which serves with, single customer whereas customer has its own independent instance of software in dedicated environment.
- 5) **Multitenant:** Accessing the services in shared environment across multiple organizations, whereas server resources are shared among different customers.

Features of Azure active directory:

- 1) Single sign-on
- 2) Self-service password administration
- 3) Identity protection
- 4) Privileged identity management

Steps to create a new tenant:

Step 1: Login to your organization's *Azure portal*

Step 2: Search for *Azure active directory* in the portal search bar.

Step 3: Select *create tenant* option.

Step 4: You will get *basics, configuration* and *review + create* tabs.

Home > Fourth Coffee >

Create a tenant

Azure Active Directory

* Basics * **Configuration** Review + create

Directory details

Configure your new directory

Organization name * ⓘ ✓

Initial domain name * ⓘ ✓
contosoorg.onmicrosoft.com

Country/Region ⓘ ✓

✓ Datacenter location - United States

Datacenter location is based on the country/region selected above.

Step 5: In the basics tab we have the option to select the type of tenant, Azure active directory or Azure active directory (B2C) you want to create, and click on next.

Step 6: In the configuration tab

- i) Organization name
- ii) Initial domain name
- iii) Country/region

Select next: Review + Create and check whether the entered information is correct or not, if its correct, click on create.

Home > Fourth Coffee >

Create a tenant

Azure Active Directory

✓ Validation passed.

* Basics * Configuration **Review + create**

Summary

Basics

Tenant type Azure Active Directory

Configuration

Organization name	Contoso Organization
Initial domain name	contosoorg.onmicrosoft.com
Country/Region	United States
Datacenter location	United States

New tenant is created successfully.

3. Azure Active Directory Domain Services:

It is also known as Azure's Managed cloud. It offers managed domain services (DS). Domain services include lightweight directory access protocol, Kerberos/NTLM authentication, group policy, and domain policy.

AADDS can integrate with our already existing Azure AD tenant. This integration enables our users using their existing usable credentials for connection to the managed domain's services. User accounts and existing groups can be used to secure access to services.

Working of Azure ADDS

On the creation of the AAD DS managed domain, a unique namespace is declared. This namespace acts as the domain name, such as verifyme.in. Following that, a pair of domain controllers such as 'Windows Server domain controllers are deployed into an Azure region which can be selected by us. This deployment of domain controllers can be called as a replica set.

These DCs don't need manage or update. Services are offered to these DCs via the Azure platform by being a managed domain's part. An example of such a service could be encryption at rest using Azure's Disk Encryption and backups.

A managed domain performs a uni-directional synchronization, starting at Azure AD and offers access to a centralized set of users, groups, and credentials. You may have resources created directly into the managed domain, but there is no synchronization towards Azure AD.

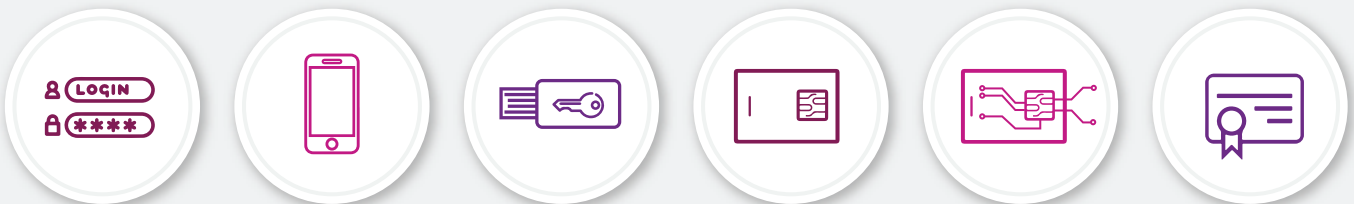
Azure AD vs Azure ADDS: a comparison

- AAD is the directory that works behind M365/O365 workloads and provides security and identity services. It's not a domain service when compared to the traditional AD.
- AAD DS service is the domain service. It offers same features compared to on-prem AD with domain joins and group policy. Further, it has a hierarchical structure with organization units.

4. Azure AD Multi-Factor Authentication

Multi-factor authentication is a process of authenticating the user during sign-in process by using an extra form type of identity. Examples could be a fingerprint scanner on phones.

If user is using password to authenticate oneself, it leaves an insecure vector of attack, which can be used by attackers. If the user password is weak or has been exposed elsewhere, then we don't know who the login user is or is it someone else i.e attacker. When we use second form of authentication, security is increased, and it is difficult for the attacker to crack the password.



Azure AD Multi-Factor Authentication follows authentication steps mentioned below:

- Using password
- Using a trusted device such as phone or hardware key
- Using biometrics like face scan/fingerprint

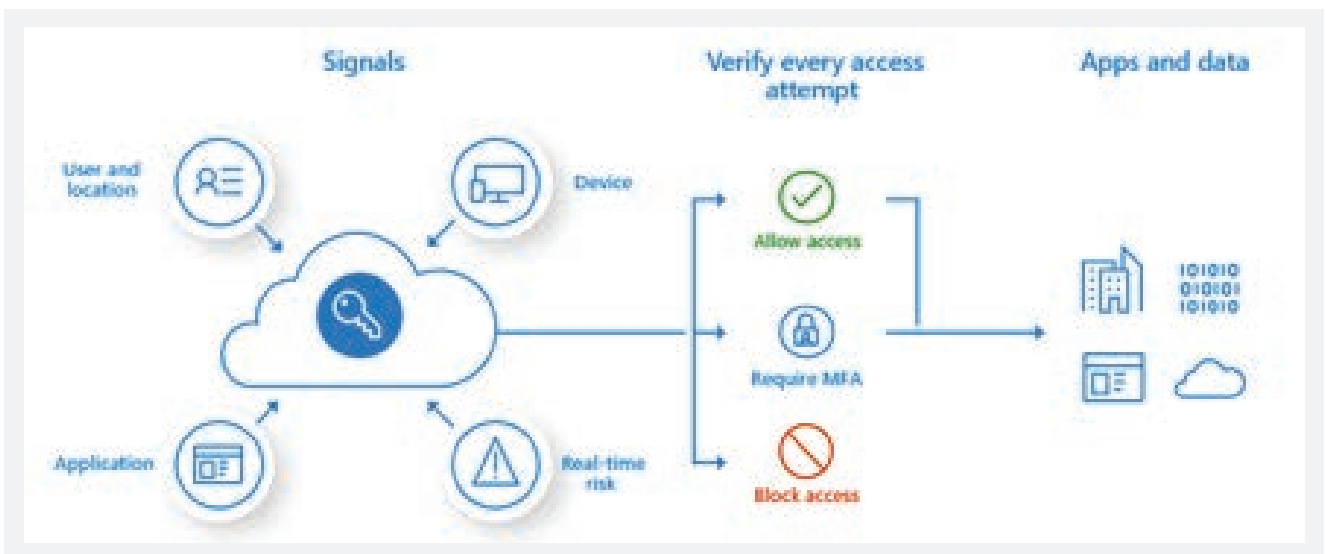
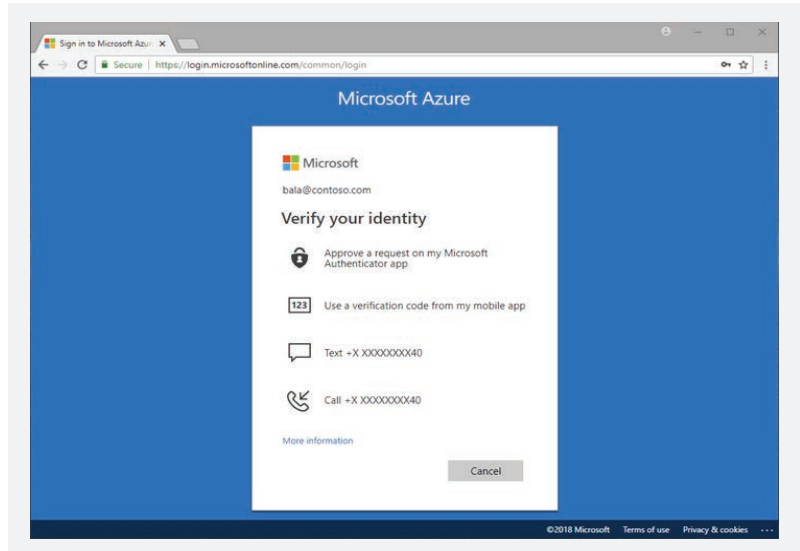
By providing strong authentication by using different methods and using second form of authentication, Azure AD Multi-Factor Authentication provides additional security.

Applications or services are not required for making any changes while configuring the Azure AD Multi-Factor Authentication. The verification leads to verifying the identity, which automatically requests and then processes the MFA challenge if required.

Enabling and using Azure AD Multi-Factor Authentication

We can configure Users and Groups in Azure AD Multi-Factor Authentication for additional verification. This security is available for all Azure AD users to use Microsoft Authenticator app for all users.

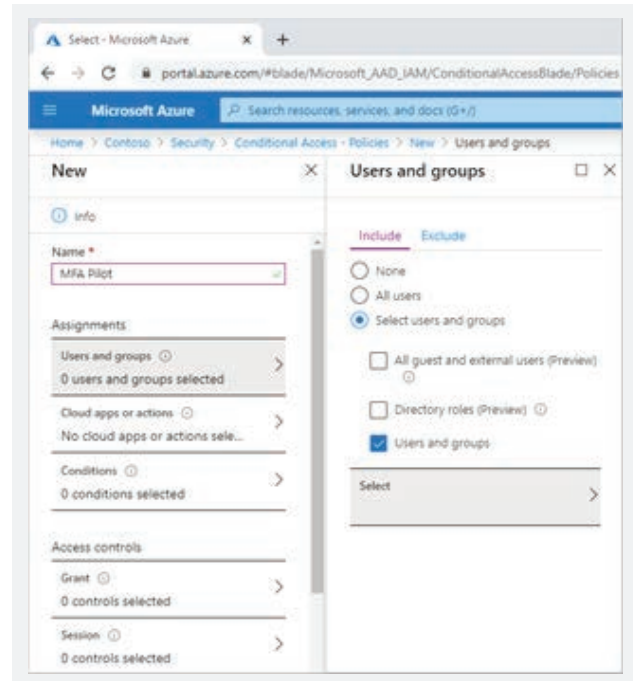
Conditional Access Policies are preferred over defined applications/events, which require Multi Factor Authentication. These policies allow the user to use registered device or corporate network, prompts for additional verification factors when on a personal device or remotely by assigning some policies.



Mindtree follows the below steps for Conditional Access Policy to assign a particular group of users:

1. Login to Azure portal with administrator permissions.
2. Search **Azure Active Directory**, and then select **Security** from the menu.
3. Select **Conditional Access**, then select **+ New policy**.
4. Give a name for the policy, i.e., MFA Pilot.
5. Then below Assignments, select groups and users.
6. After that, select on preferred groups and users buttons.

7. Tick up the check box for groups and users.
8. Further Select Azure AD group, i.e. MFA-Test-Group, then click **Select**.
9. To apply the Conditional Access policy for the group, click **Done**.
10. To apply the Conditional Access policy for the group, click **Done**.

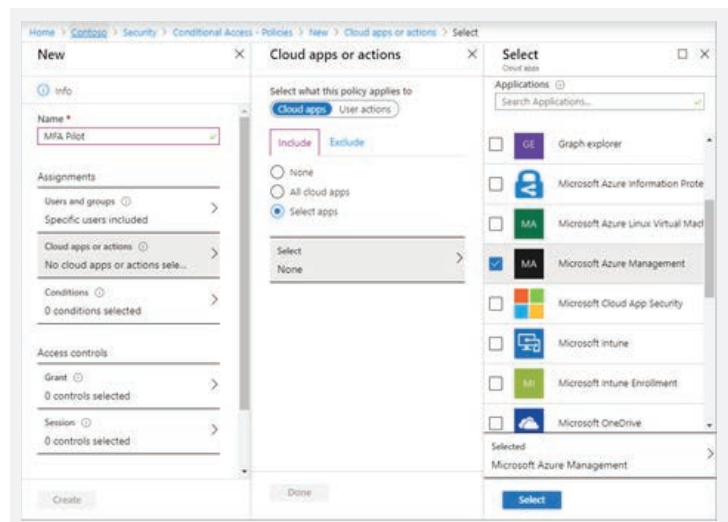


Configuring conditions for multi-factor authentication

Condition policy for particular users and groups can be used. With conditional policy, we can also use MFA prompt for additional security. For Example, the application of use of any tool requires an additional verification prompt.

Below steps are followed by Mindtree for Conditional Access Policy to require MFA when a user logs in to the Azure Portal:

1. Under Assignments, Select Cloud apps or actions. Then, Select the Conditional Access policy to all cloud apps or Select apps. For this on the Include page, click on Select apps radio button.
2. Select, and then browse the list of available sign-in events, which we can use for security. Then, Select Microsoft Azure Management so that the policy applies to sign-in events to the Azure portal.
3. To apply on select apps, click Select, then Done.



Access controls lets us prepare the specifications for granting access to a user. In this configuration, the access ensures that an MFA is needed for events of sign-in types into the Azure portal.

1. For Access controls, select Grant. Next ensure that Grant access radio button is ticked up.
2. Check the box for **Require multi-factor authentication**, then click on **Select**. Conditional Access policies can be adjusted.

Use it in Report-only mode if your aim is to observe how users will be affected by configuration.

Use it in off mode if policy usage is not needed. Let's enable the policy and then test Azure AD MFA.

1. Keep the policy called enable flipping to on.
2. Select **Create**, if all you need is the application of Conditional Access policy

Call to action

For more information about Identity and Access management on Azure security Services please use the below links:

<https://docs.microsoft.com/en-us/Azure/role-based-access-control/role-assignments-portal>

<https://docs.microsoft.com/en-us/Azure/active-directory/fundamentals/active-directory-what-is>

<https://docs.microsoft.com/en-us/Azure/active-directory-domain-services/overview>

<https://docs.microsoft.com/en-us/Azure/active-directory/authentication/concept-mfa-how-it-works>

About Mindtree

Mindtree [NSE: MINDTREE] is a global technology consulting and services company, helping enterprises marry scale with agility to achieve competitive advantage. "Born digital," in 1999 and now a Larsen & Toubro Group Company, Mindtree applies its deep domain knowledge to 270 enterprise client engagements to break down silos, make sense of digital complexity and bring new initiatives to market faster. We enable IT to move at the speed of business, leveraging emerging technologies and the efficiencies of Continuous Delivery to spur business innovation. Operating in 24 countries across the world, we are consistently regarded as one of the best places to work, embodied every day by our winning culture made up of over 23,800 entrepreneurial, collaborative and dedicated "Mindtree Minds."