

Attention students:

In order to demonstrate successful completion of all components in the project, please use screenshot(s) to show each completed action step as specified on the instructions page.

Identity and Access Management

1. Proof of Assigned roles and AD assignments

Andrew-neelima-neha-seth-srinadh-tom-winfred

Microsoft Azure portal showing the 'IT' group overview page. The page displays group properties such as Membership type (Assigned), Source (Cloud), Type (Security), and Object Id (2f05f3ae-578e-41dc-b6c2-3bce6eb38c94). It also shows a summary of members: 12 Total (12 User(s), 0 Group(s), 0 Device(s), 0 Other(s)).

Microsoft Azure portal showing the 'IT' group members page. The page displays a list of 12 members with columns for Name, Type, Email, and User type. The members listed are Andrew, Debora, Doug, Michael, Neelima, Neha, Rajiv, Sean, Seth, Srinadh, Tom, and Winifred, all of whom are Users.

Name	Type	Email	User type
<input type="checkbox"/> AN Andrew	User		Member
<input type="checkbox"/> DE Debora	User		Member
<input type="checkbox"/> DO Doug	User		Member
<input type="checkbox"/> MI Michael	User		Member
<input type="checkbox"/> NE Neelima	User		Member
<input type="checkbox"/> NE Neha	User		Member
<input type="checkbox"/> RA Rajiv	User		Member
<input type="checkbox"/> SE Sean	User		Member
<input type="checkbox"/> SE Seth	User		Member
<input type="checkbox"/> SR Srinadh	User		Member
<input type="checkbox"/> TO Tom	User		Member
<input type="checkbox"/> WI Winifred	User		Member

IT - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~/AdministrativeRole/groupId/2f05f3ae-578e-41dc-b6c2-3bce6eb38c94

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208236@d4ud... UDACITY 1014 (CLAUDACTY1014...)

Home > Groups | All groups > IT

IT | Assigned roles

Group

- Overview
- Diagnose and solve problems
- Manage
 - Properties
 - Members
 - Owners
 - Roles and administrators
 - Administrative units
 - Group memberships
 - Assigned roles
 - Applications
 - Licenses
 - Azure role assignments
- Activity
 - Privileged access (Preview)
 - Access reviews
 - Audit logs
 - Bulk operation results
- Troubleshooting + Support

+ Add assignments Refresh Got feedback?

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...		Directory	Direct	Active	-	Permanent	Remove Update

executives - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~/Overview/groupId/ee9d6435-da37-48b9-8aed-5c9c6f24e17a

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208236@d4ud... UDACITY 1014 (CLAUDACTY1014...)

Home > Groups | All groups > executives

executives

Group

- Overview
- Diagnose and solve problems
- Manage
 - Properties
 - Members
 - Owners
 - Roles and administrators
 - Administrative units
 - Group memberships
 - Assigned roles
 - Applications
 - Licenses
 - Azure role assignments
- Activity
 - Privileged access (Preview)
 - Access reviews
 - Audit logs
 - Bulk operation results
- Troubleshooting + Support

Delete Got feedback?

EX executives
executives members

Membership type: Assigned

Source: Cloud

Type: Security

Object id: ee9d6435-da37-48b9-8aed-5c9c6f24e17a

Created at: 9/21/2022, 11:41:15 PM

Counts may be inaccurate if this group was recently created.

Direct members: 0 User(s), 0 Group(s), 0 Device(s), 0 Other(s)

Group memberships: 0, Owners: 0, Total members: 0

executives - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~/Members/groupId/ee9d6435-da37-48b9-8aed-5c9c6f24e17a

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > executives

executives | Members

Group

- Overview
- Diagnose and solve problems
- Manage
 - Properties
 - Members**
 - Owners
 - Roles and administrators
 - Administrative units
 - Group memberships
 - Assigned roles
 - Applications
 - Licenses
 - Azure role assignments
- Activity
 - Privileged access (Preview)
 - Access reviews
 - Audit logs
 - Bulk operation results
- Troubleshooting + Support

+ Add members Remove Refresh Bulk operations Columns Got feedback?

Direct members All members

Search by name Add filters

	Name	Type	Email	User type
<input type="checkbox"/>	CH Chris	User		Member
<input type="checkbox"/>	KA Karl	User		Member

executives - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~/AdministrativeRole/groupId/ee9d6435-da37-48b9-8aed-5c9c6f24e17a

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > executives

executives | Assigned roles

Group

- Overview
- Diagnose and solve problems
- Manage
 - Properties
 - Members
 - Owners
 - Roles and administrators
 - Administrative units
 - Group memberships
 - Assigned roles**
 - Applications
 - Licenses
 - Azure role assignments
- Activity
 - Privileged access (Preview)
 - Access reviews
 - Audit logs
 - Bulk operation results
- Troubleshooting + Support

+ Add assignments Refresh Got feedback?

Eligible assignments **Active assignments** Expired assignments

Search by role

	Role	Principal name	Scope	Membership	State	Start time	End time	Action
	Message Center Rea...		Directory	Direct	Active	-	Permanent	Remove Update

HR - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~//Overview/groupId/172c90a0-fbeb-4381-b948-9e652eb4a719

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups >

HR
Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Assigned roles
- Applications
- Licenses
- Azure role assignments

Activity

- Privileged access (Preview)
- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

Delete | Got feedback?

HR
Human Resources Members

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: 172c90a0-fbeb-4381-b948-9e652eb4a719

Created at: 9/22/2022, 12:22:14 AM

Direct members

2 Total: 2 User(s), 0 Group(s), 0 Device(s), 0 Other(s)

Group memberships: 0, Owners: 0, Total members: 2

HR - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_IAM/GroupDetailsMenuBlade/~//Members/groupId/172c90a0-fbeb-4381-b948-9e652eb4a719

Microsoft Azure Search resources, services, and docs (G+)

Home > Groups | All groups > HR

HR | Members
Group

Overview

Diagnose and solve problems

Manage

- Properties
- Members
- Owners
- Roles and administrators
- Administrative units
- Group memberships
- Assigned roles
- Applications
- Licenses
- Azure role assignments

Activity

- Privileged access (Preview)
- Access reviews
- Audit logs
- Bulk operation results

Troubleshooting + Support

+ Add members | Remove | Refresh | Bulk operations | Columns | Got feedback?

Direct members | All members

Search by name: Add filters

Name	Type	Email	User type
<input type="checkbox"/> KA Kaitlyn	User		Member
<input type="checkbox"/> LO Lora	User		Member

HR | Assigned roles

- Overview
- Diagnose and solve problems
- Manage
 - Properties
 - Members
 - Owners
 - Roles and administrators
 - Administrative units
 - Group memberships
 - Assigned roles**
 - Applications
 - Licenses
 - Azure role assignments
- Activity
 - Privileged access (Preview)
 - Access reviews
 - Audit logs
 - Bulk operation results
- Troubleshooting + Support

+ Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
User Administrator		Directory	Direct	9/22/2022, 12:24:14 AM	9/22/2023, 12:23:33 AM	Remove Update Exten

a. Andrew

Andrew | Assigned roles

Search resources, services, and docs (G+)

Home > Users > Andrew

Andrew | Assigned roles

Search

+ Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...	Andrew@cl4udacity1...	Directory	Group	Active	-	Permanent	Remove Update

Management options: Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Custom security attributes (preview), Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods, Troubleshooting + Support, New support request.

Andrew | Azure role assignments

Search resources, services, and docs (G+)

Home > Users > Andrew

Andrew | Azure role assignments

Search

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

Subscription *
Udacity 1021

Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	VNet-prod	Virtual network	Andrew	None
Contributor	Vnet-operations	Virtual network	Andrew	None

Management options: Overview, Audit logs, Sign-in logs, Diagnose and solve problems, Custom security attributes (preview), Assigned roles, Administrative units, Groups, Applications, Licenses, Devices, Azure role assignments, Authentication methods, Troubleshooting + Support, New support request.

b. Chris

Chris - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade~/AdministrativeRole/userId/9c02a722-26d8-4074-b8ab-b6981bf3ca93

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Chris

Chris | Assigned roles

Search

+ Add assignments Refresh Got feedback?

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...	Chris@cl4udacity101...	Directory	Group	Active	-	Permanent	Remove Update

Manage

- Custom security attributes (preview)
- Assigned roles**
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

Chris - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade~/AdministrativeRole/userId/edd5107d-c33b-47b2-9097-603b8fd7e702

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Chris

Chris | Assigned roles

Search

+ Add assignments Refresh Got feedback?

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
Global Administrator	Chris@cl4udacity1021.o...	Directory	Direct	9/23/2022, 6:01:51 PM	Permanent	Remove Update
Billing Administrator	Chris@cl4udacity1021.o...	Directory	Direct	9/23/2022, 6:02:11 PM	Permanent	Remove Update

Manage

- Custom security attributes (preview)
- Assigned roles**
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

c. Karl

Karl - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade~/AdministrativeRole/userId/3aa24adb-35d2-473d-a755-4d42e4b8ff09

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Karl

Karl | Assigned roles

User

Search << + Add assignments Refresh Got feedback?

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods

Troubleshooting + Support
New support request

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...	Karl@cl4udacity1014...	Directory	Group	Active	-	Permanent	Remove Update
Billing Administrator	Karl@cl4udacity1014...	Directory	Direct	Active	9/21/2022, 11:59:08 ...	Permanent	Remove Update

d. Lora

Lora - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade~/AdministrativeRole/userId/f0d8c916-ab12-4e1a-b00a-8ae1aea5b8f0

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Lora

Lora | Assigned roles

User

Search << + Add assignments Refresh Got feedback?

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods

Troubleshooting + Support
New support request

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
User Administrator	Lora@cl4udacity1014.on...	Directory	Group	9/22/2022, 12:24:14 AM	9/22/2023, 12:23:33 AM	Remove Update Exten

e. Neelima

Neelima - Microsoft Azure | Cloud Device Administrator - M...

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/0e64780a-58e8-431a-a53f-adfb9e27a241

Microsoft Azure | Search resources, services, and docs (G+)

Home > Users > Neelima

Neelima | Assigned roles

User

Search << + Add assignments Refresh | Got feedback?

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

Eligible assignments | **Active assignments** | Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Azure DevOps Admi...	Neelima@cl4udacity...	Directory	Direct	Active	9/23/2022, 6:17:07 PM	Permanent	Remove Update
Cloud Device Admini...	Neelima@cl4udacity...	Directory	Direct	Active	9/23/2022, 6:16:11 PM	Permanent	Remove Update
Message Center Rea...	Neelima@cl4udacity...	Directory	Group	Active	-	Permanent	Remove Update

Neelima - Microsoft Azure | +

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_SubscriptionResources/userId/0e64780a-58e8-431a-a53f-adfb9e27a241

Microsoft Azure | Search resources, services, and docs (G+)

Home > Users > Neelima

Neelima | Azure role assignments

User

Search <<

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *
Udacity 1021

Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	Vnet-Dev	Virtual network	Neelima	None
Contributor	sql-devdata-208323	SQL server	Neelima	None
Contributor	sql-proddata-208323	SQL server	Neelima	None
Reader	sql-devdata-208323	SQL server	Neelima	None
Reader	sql-proddata-208323	SQL server	Neelima	None

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

f. Neha

Microsoft Azure portal: Assigned roles for user Neha.

Navigation: Home > Users > Neha

Search: Search resources, services, and docs (G+)

Assigned roles for Neha (User):

- Overview
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Manage
 - Custom security attributes (preview)
 - Assigned roles**
 - Administrative units
 - Groups
 - Applications
 - Licenses
 - Devices
 - Azure role assignments
 - Authentication methods
- Troubleshooting + Support
 - New support request

Eligible assignments | **Active assignments** | Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Azure DevOps Admi...	Neha@cl4udacity10...	Directory	Direct	Active	9/23/2022, 6:19:43 PM	Permanent	Remove Update
Message Center Rea...	Neha@cl4udacity10...	Directory	Group	Active	-	Permanent	Remove Update

Microsoft Azure portal: Azure role assignments for user Neha.

Navigation: Home > Users > Neha

Search: Search resources, services, and docs (G+)

Azure role assignments for Neha (User):

- Overview
- Audit logs
- Sign-in logs
- Diagnose and solve problems
- Manage
 - Custom security attributes (preview)
 - Assigned roles
 - Administrative units
 - Groups
 - Applications
 - Licenses
 - Devices
 - Azure role assignments**
 - Authentication methods
- Troubleshooting + Support
 - New support request

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *
Udacity 1021

Role	Resource Name	Resource Type	Assigned To	Condition
Reader	sql-devdata-208323	SQL server	Neha	None
Reader	sql-proddata-208323	SQL server	Neha	None

g. Seth

Seth - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/92a4a7c7-5942-426d-aae8-70cf75e6ebbe

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Seth

Seth | Assigned roles

User

Search

+ Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...	Seth@cl4udacity101...	Directory	Group	Active	-	Permanent	Remove Update

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

New support request

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/92a4a7c7-5942-426d-aae8-70cf75e6ebbe

Seth - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/92a4a7c7-5942-426d-aae8-70cf75e6ebbe

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Seth

Seth | Assigned roles

User

Search

+ Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
Global Administrator	Seth@cl4udacity1014.on...	Directory	Direct	9/22/2022, 12:03:00 AM	Permanent	Remove Update
Billing Administrator	Seth@cl4udacity1014.on...	Directory	Direct	9/22/2022, 12:03:20 AM	Permanent	Remove Update

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

New support request

h. Srinadh

Srinadh - Microsoft Azure | Cloud Device Administrator - Mi: x +

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade~/AdministrativeRole/userId/7bbbd9c0-a657-474e-a5bc-ca977a86af00

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Srinadh

Srinadh | Assigned roles

User

Search Add assignments Refresh Got feedback?

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Azure DevOps Admi...	Srinadh@cl4udacity1...	Directory	Direct	Active	9/23/2022, 6:21:33 PM	Permanent	Remove Update
Message Center Rea...	Srinadh@cl4udacity1...	Directory	Group	Active	-	Permanent	Remove Update

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

Srinadh - Microsoft Azure | +

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade~/SubscriptionResources/userId/7bbbd9c0-a657-474e-a5bc-ca977a86af00

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Srinadh

Srinadh | Azure role assignments

User

Search

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. Learn more

Subscription *
Udacity 1021

Role	Resource Name	Resource Type	Assigned To	Condition
Reader	sql-devdata-208323	SQL server	Srinadh	None
Reader	sql-proddata-208323	SQL server	Srinadh	None

Manage

- Custom security attributes (preview)
- Assigned roles
- Administrative units
- Groups
- Applications
- Licenses
- Devices
- Azure role assignments
- Authentication methods

Troubleshooting + Support

- New support request

i. Tom

Tom - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/f33ef96c-fa65-4817-bece-cbc91aa20eff

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Tom

Tom | Assigned roles ...

User

Search Add assignments Refresh Got feedback?

Eligible assignments **Active assignments** Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...	Tom@d4udacity101...	Directory	Group	Active	-	Permanent	Remove Update

https://portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlad...

Tom - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_SubscriptionResources/userId/39ffd562-3eb5-4c67-88d9-d6fb1b72cf01

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Tom

Tom | Azure role assignments ...

User

Search

If this identity has role assignments that you don't have permission to read, they won't be shown in the list. [Learn more](#)

Subscription *
Udacity 1021

Role	Resource Name	Resource Type	Assigned To	Condition
Contributor	VNet-prod	Virtual network	Tom	None
Contributor	Vnet-operations	Virtual network	Tom	None

j. Winifred

Winifred - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/86abefb9-f70c-4ce2-b8b8-3367380a471c

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Winifred

Winifred | Assigned roles

User

Search Add assignments Refresh Got feedback?

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods

Troubleshooting + Support
New support request

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	Start time	End time	Action
Helpdesk Administrator	Winifred@cl4udacity101...	Directory	Direct	9/21/2022, 11:26:48 PM	Permanent	Remove Update

Winifred - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_UsersAndTenants/UserProfileMenuBlade/~/_AdministrativeRole/userId/86abefb9-f70c-4ce2-b8b8-3367380a471c

Microsoft Azure Search resources, services, and docs (G+)

Home > Users > Winifred

Winifred | Assigned roles

User

Search Add assignments Refresh Got feedback?

Overview
Audit logs
Sign-in logs
Diagnose and solve problems

Manage
Custom security attributes (preview)
Assigned roles
Administrative units
Groups
Applications
Licenses
Devices
Azure role assignments
Authentication methods

Troubleshooting + Support
New support request

Eligible assignments Active assignments Expired assignments

Search by role

Role	Principal name	Scope	Membership	State	Start time	End time	Action
Message Center Rea...	Winifred@cl4udacity...	Directory	Group	Active	-	Permanent	Remove Update

2. Proof of Global Administrator setting with duration, eligibility, expiration

Microsoft Azure portal interface showing the "Edit role setting - Global Administrator" page. The page is under the "Activation" tab. The "Activation maximum duration (hours)" is set to 8. The "On activation, require" options are "None" and "Azure MFA" (selected). Other options include "Require justification on activation" (checked), "Require ticket information on activation" (unchecked), and "Require approval to activate" (unchecked). A search bar for approver(s) shows "No approver selected". Buttons at the bottom include "Update" and "Next: Assignment".

Microsoft Azure portal interface showing the "Edit role setting - Global Administrator" page. The page is under the "Assignment" tab. The "Allow permanent eligible assignment" checkbox is unchecked. The "Expire eligible assignments after" dropdown is set to "1 Year". The "Allow permanent active assignment" checkbox is unchecked. The "Expire active assignments after" dropdown is set to "6 Months". The "Require Azure Multi-Factor Authentication on active assignment" and "Require justification on active assignment" checkboxes are checked. Buttons at the bottom include "Update", "Prev: Activation", and "Next: Notification".

Role setting details - Global Administrator

Privileged Identity Management | Azure AD roles

[Edit](#)

Activation

Setting	State
Activation maximum duration (hours)	8 hour(s)
Require justification on activation	Yes
Require ticket information on activation	No
On activation, require Azure MFA	Yes
Require approval to activate	No
Approvers	None

Assignment

Setting	State
Allow permanent eligible assignment	No
Expire eligible assignments after	1 year(s)
Allow permanent active assignment	No
Expire active assignments after	6 month(s)
Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

Send notifications when members are assigned as eligible to this role:

Role setting details - Global Administrator

Privileged Identity Management | Azure AD roles

[Edit](#)

Require Azure Multi-Factor Authentication on active assignment	Yes
Require justification on active assignment	Yes

Send notifications when members are assigned as eligible to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	-	None	False
Notification to the assigned user (assignee)	-	None	False
Request to approve a role assignment renewal/extens...	-	None	False

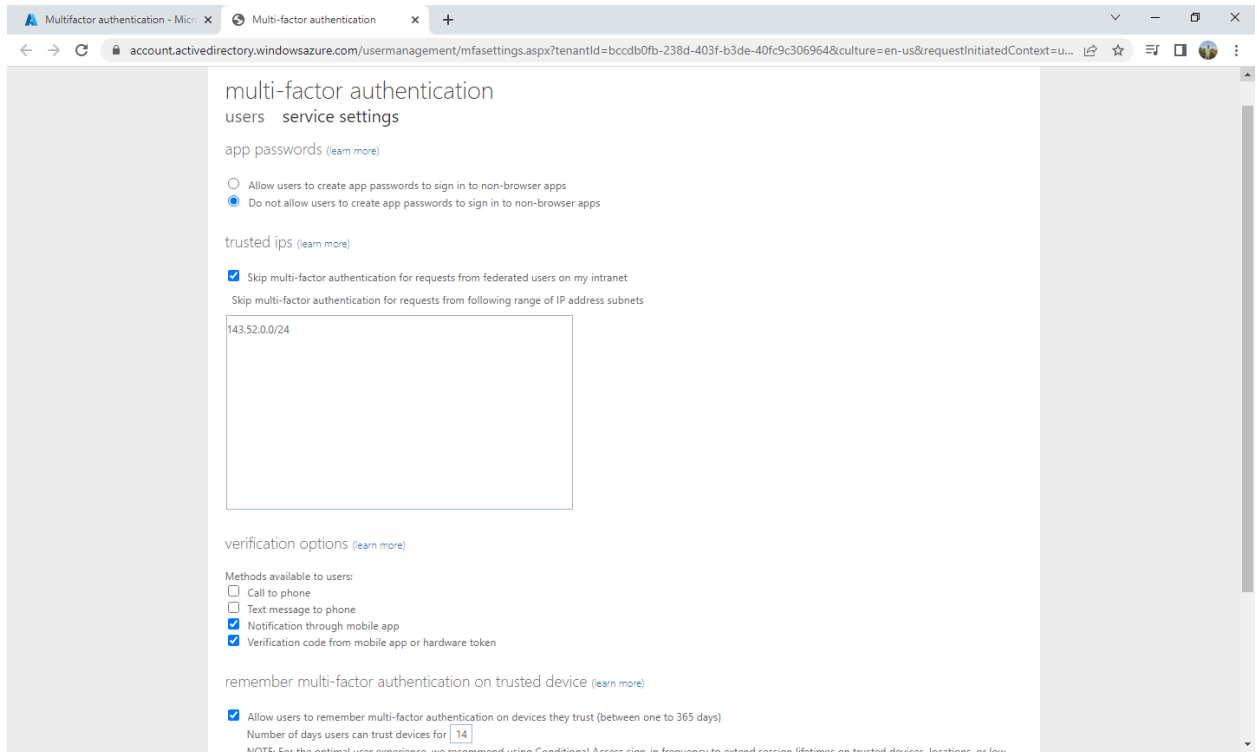
Send notifications when members are assigned as active to this role:

Type	Default recipients	Additional recipients	Critical emails only
Role assignment alert	-	None	False
Notification to the assigned user (assignee)	-	None	False
Request to approve a role assignment renewal/extens...	-	None	False

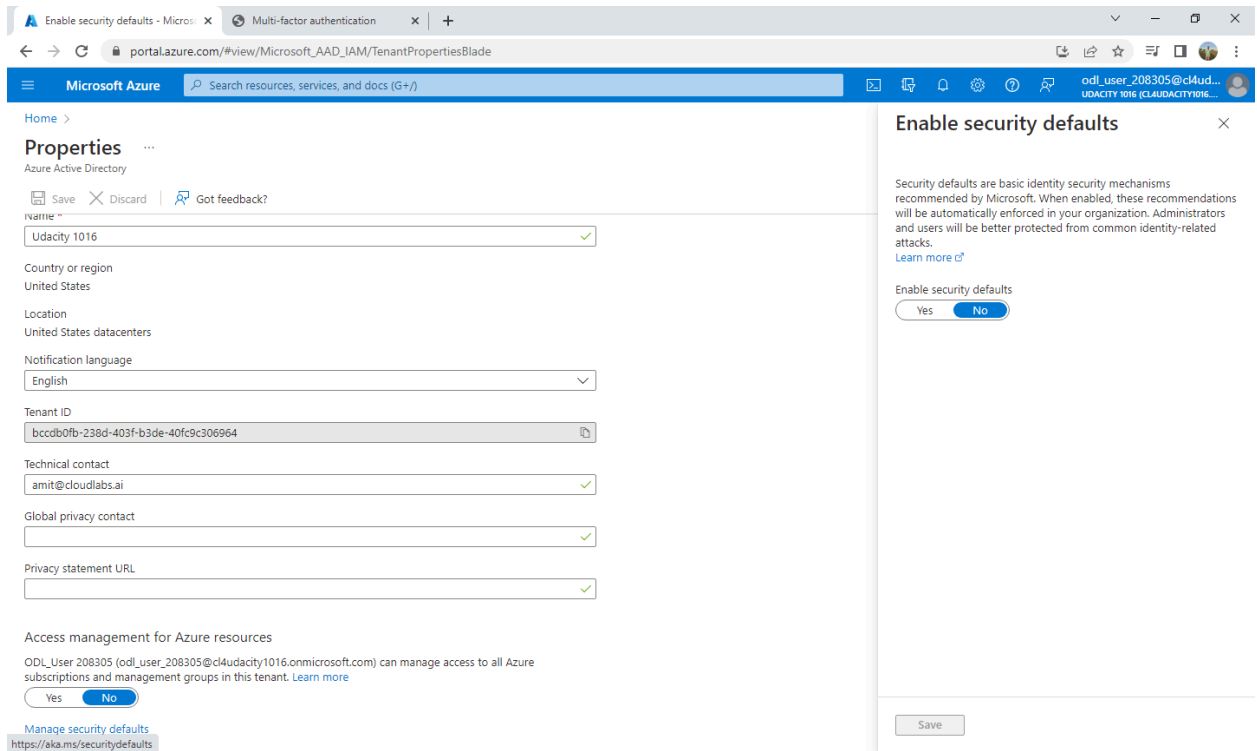
Send notifications when eligible members activate this role:

Type	Default recipients	Additional recipients	Critical emails only
Role activation alert	-	None	False
Notification to activated user (requestor)	-	None	False
Request to approve an activation	-	None	False

3. Proof of Conditional Access policy all users



Making sure that we disabled the security defaults



Microsoft Azure | Search resources, services, and docs (G+)

Home > Conditional Access | Policies >

All Users MFA

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests. [Learn more](#)

Name *
All Users MFA

What does this policy apply to?
Users and groups

Assignments

Users or workload identities ⓘ
All users included and specific users excluded

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
1 control selected

Enable policy
Report-only On Off

Save

<https://aka.ms/CaUsersGroups>

Warning: Don't lock yourself out! This policy will affect all of your users. We recommend applying a policy to a small set of users first to verify it behaves as expected.

Microsoft Azure | Search resources, services, and docs (G+)

Home > Conditional Access | Policies >

All Users MFA

Conditional Access policy

Delete

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on all or specific cloud apps or actions. [Learn more](#)

Select what this policy applies to
Cloud apps User actions
Authentication context (preview)

Assignments

Users or workload identities ⓘ
All users included and specific users excluded

Cloud apps or actions ⓘ
All cloud apps

Conditions ⓘ
0 conditions selected

Access controls

Grant ⓘ
1 control selected

Enable policy
Report-only On Off

Save

<https://aka.ms/CaCloudActionsAuths>

Warning: Don't lock yourself out! This policy impacts the Azure portal. Before you continue, ensure that you or someone else will be able to get back into the portal. Disregard this warning if you are configuring persistent browser session policy that works correctly only if "All cloud apps" are selected.

Grant - Microsoft Azure

portal.azure.com/#view/Microsoft_AAD_ConditionalAccess/PolicyBlade/policyid/300f3932-ada8-4427-8d96-b84a73163bee/applid~/null/policyName~/null

Home > Conditional Access | Policies > All Users MFA

Conditional Access policy

Delete

Name *

All Users MFA

Assignments

Users or workload identities

All users included and specific users excluded

Cloud apps or actions

All cloud apps

Conditions

0 conditions selected

Access controls

Grant

1 control selected

Session

0 controls selected

Enable policy

Report-only On Off

Save

https://aka.ms/capolicygrant

Grant

Control access enforcement to block or grant access. [Learn more](#)

Block access

Grant access

Require multifactor authentication

Require device to be marked as compliant

Require Hybrid Azure AD joined device

Require approved client app

[See list of approved client apps](#)

Require app protection policy

[See list of policy protected client apps](#)

Require password change

For multiple controls

Require all the selected controls

Require one of the selected controls

Select

4. Proof of Multi-factor authentication(14 days, Charlotte office info)

Multi-factor authentication - Micr

Multi-factor authentication

account.activedirectory.windowsazure.com/usermanagement/mfasettings.aspx?tenantid=bcceb0fb-238d-403f-b3de-40fc9c306964&culture=en-us&requestInitiatedContext=u...

multi-factor authentication

users service settings

app passwords [\(learn more\)](#)

Allow users to create app passwords to sign in to non-browser apps

Do not allow users to create app passwords to sign in to non-browser apps

trusted ips [\(learn more\)](#)

Skip multi-factor authentication for requests from federated users on my intranet

Skip multi-factor authentication for requests from following range of IP address subnets

143.52.0.0/24

verification options [\(learn more\)](#)

Methods available to users:

Call to phone

Text message to phone

Notification through mobile app

Verification code from mobile app or hardware token

remember multi-factor authentication on trusted device [\(learn more\)](#)

Allow users to remember multi-factor authentication on devices they trust (between one to 365 days)

Number of days users can trust devices for 14

NOTE: For the optimal user experience, we recommend using Conditional Access in conjunction with device compliance on trusted devices. For more information, see [Device compliance](#).

Network Security

1. Bastion overview

Validation passed

Basics Tags Advanced **Review + create**

Summary

Basics

Name	bastion-project
Subscription	Udacity 1021
Resource group	rg-core
Region	East US
Virtual network	VNet-core
Subnets	AzureBastionSubnet
Public IP address	VNet-core-ip
Tier	Standard
Instance count	2
Copy and paste	Enabled
IP-based connection	Disabled
Kerberos authentication (Preview)	Disabled
Native client support	Disabled

[Create](#) [Previous](#) [Next](#) [Download a template for automation](#)

bastion-project Bastion

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Sessions
- Configuration
- Properties
- Locks

Monitoring

- Metrics
- Logs
- Diagnostics settings
- Connection Troubleshoot

Automation

- Tasks (preview)
- Export template

Essentials

Resource group (move)	Virtual network/subnet
rg-core	VNet-core/AzureBastionSubnet
Location	Public DNS name
East US	-
Subscription (move)	Public IP address
Udacity 1021	VNet-core-ip
Subscription ID	Tier
2c66b487-2f2e-48cd-9374-92db8d0ec2d2	Standard
	Provisioning state
	Updating

Tags ([edit](#))
[Click here to add tags](#)

Sessions Tutorials

SessionId	StartTime (UTC)	TargetSubscriptionId	ResourceType	TargetHostName	TargetResourceGr
Unable to get the sessions for the Bastion, please try again.					

Page 1 of 1

2. Proof of public IP addresses removed

The screenshot displays the Azure portal interface for a virtual machine named 'vm-ws16devapp'. The 'Essentials' section provides a summary of the VM's state and configuration:

- Resource group:** rg-dev
- Operating system:** Windows
- Status:** Stopped (deallocated)
- Size:** Standard B2s (2 vcpus, 4 GiB memory)
- Location:** East US
- Subscription:** Udacity 1021
- Subscription ID:** 2c66b487-2f2e-48cd-9374-92db8d0ec2d2
- Virtual network/subnet:** Vnet-Dev/default
- Tags:** (None listed)

The 'Networking' section shows the following IP addresses:

Category	Value
Public IP address	-
Public IP address (IPv6)	-
Private IP address	10.2.0.4
Private IP address (IPv6)	-

The 'Virtual machine' section shows the following details:

Property	Value
Computer name	VM-WS16DevWeb
Health state	-
Operating system	Windows
Publisher	MicrosoftWindowsServer
Offer	WindowsServer

VM-WS16DevWeb - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-dev/providers/Microsoft.Compute/virtualMachines/VM-WS16DevWeb

Home > Virtual machines > Virtual machines

Virtual machines
Udacity 1021 (cl4udacity1021.onmicrosoft.com)

+ Create ▾ Switch to classic ...

Filter for any field...

Name ↑

- vm-ws16devapp
- VM-WS16DevWeb**
- VM-WS16OpWeb
- VM-WS19HRL-App
- VM-WS19HRL-Web
- VM-WS19OpApp

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center (preview)
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity

Connect ▾ Start ▾ Restart ▾ Stop Capture Delete Refresh Open in mobile CLI / PS

Essentials

Resource group (move) [rg-dev](#) Operating system: Windows

Status: Stopped (deallocated) Size: Standard B2s (2 vcpus, 4 GiB memory)

Location: East US Public IP address: -

Subscription (move) [Udacity 1021](#) Virtual network/subnet: [Vnet-Dev/default](#)

Subscription ID: 2c66b487-2f2e-48cd-9374-92db8d0ec2d2 DNS name: -

Tags (edit) [Click here to add tags](#)

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	VM-WS16DevWeb	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows	Private IP address	10.2.0.5
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer		

Networking

Public IP address -

Public IP address (IPv6) -

Private IP address 10.2.0.5

Private IP address (IPv6) -

Page 1 of 1

[Give feedback](#)

VM-WS16OpWeb - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-operations/providers/Microsoft.Compute/virtualMachines/VM-WS16OpWeb

Home > Virtual machines > Virtual machines

Virtual machines
Udacity 1021 (cl4udacity1021.onmicrosoft.com)

+ Create ▾ Switch to classic ...

Filter for any field...

Name ↑

- vm-ws16devapp
- VM-WS16DevWeb
- VM-WS16OpWeb**
- VM-WS19HRL-App
- VM-WS19HRL-Web
- VM-WS19OpApp

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center (preview)
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity

Connect ▾ Start ▾ Restart ▾ Stop Capture Delete Refresh Open in mobile CLI / PS

Essentials

Resource group (move) [rg-operations](#) Operating system: Windows

Status: Stopped (deallocated) Size: Standard DS2 v2 (2 vcpus, 7 GiB memory)

Location: East US Public IP address: -

Subscription (move) [Udacity 1021](#) Virtual network/subnet: [Vnet-operations/default](#)

Subscription ID: 2c66b487-2f2e-48cd-9374-92db8d0ec2d2 DNS name: -

Tags (edit) [Click here to add tags](#)

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Computer name	VM-WS16OpWeb	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows	Private IP address	10.0.0.5
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer		

Networking

Public IP address -

Public IP address (IPv6) -

Private IP address 10.0.0.5

Private IP address (IPv6) -

Page 1 of 1

[Give feedback](#)

VM-WS19HRL-App - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-hrlegal/providers/Microsoft.Compute/virtualMachines/VM-WS19HRL-App

Home > Virtual machines > Virtual machines

Virtual machines

Udacity 1021 (cl4udacity1021.onmicrosoft.com)

+ Create Switch to classic

Filter for any field...

Name	...
vm-ws16devapp	...
VM-WS16DevWeb	...
VM-WS16OpWeb	...
VM-WS19HRL-App	...
VM-WS19HRL-Web	...
VM-WS19OpApp	...

Page 1 of 1

VM-WS19HRL-App

Virtual machine

Connect Start Restart Stop Capture Delete Refresh Open in mobile CLI / PS

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center (preview)
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity

Essentials

Resource group (move) [rg-hrlegal](#)

Status Stopped (deallocated)

Location East US

Subscription (move) [Udacity 1021](#)

Subscription ID 2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Tags (edit) [Click here to add tags](#)

Operating system Windows

Size Standard B2s (2 vcpus, 4 GiB memory)

Public IP address -

Virtual network/subnet [HRLegal/default](#)

DNS name -

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Property	Value	Networking	Value
Computer name	VM-WS19HRL-Web	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows	Private IP address	10.0.0.5
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer		

Give feedback

VM-WS19HRL-Web - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-hrlegal/providers/Microsoft.Compute/virtualMachines/VM-WS19HRL-Web

Home > Virtual machines > Virtual machines

Virtual machines

Udacity 1021 (cl4udacity1021.onmicrosoft.com)

+ Create Switch to classic

Filter for any field...

Name	...
vm-ws16devapp	...
VM-WS16DevWeb	...
VM-WS16OpWeb	...
VM-WS19HRL-App	...
VM-WS19HRL-Web	...
VM-WS19OpApp	...

Page 1 of 1

VM-WS19HRL-Web

Virtual machine

Connect Start Restart Stop Capture Delete Refresh Open in mobile CLI / PS

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Networking
- Connect
- Windows Admin Center (preview)
- Disks
- Size
- Microsoft Defender for Cloud
- Advisor recommendations
- Extensions + applications
- Continuous delivery
- Availability + scaling
- Configuration
- Identity

Essentials

Resource group (move) [rg-hrlegal](#)

Status Stopped (deallocated)

Location East US

Subscription (move) [Udacity 1021](#)

Subscription ID 2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Tags (edit) [Click here to add tags](#)

Operating system Windows

Size Standard B2s (2 vcpus, 4 GiB memory)

Public IP address -

Virtual network/subnet [HRLegal/default](#)

DNS name -

Properties Monitoring Capabilities (8) Recommendations Tutorials

Virtual machine

Property	Value	Networking	Value
Computer name	VM-WS19HRL-Web	Public IP address	-
Health state	-	Public IP address (IPv6)	-
Operating system	Windows	Private IP address	10.0.0.4
Publisher	MicrosoftWindowsServer	Private IP address (IPv6)	-
Offer	WindowsServer		

Give feedback

The screenshot shows the Azure portal interface for a virtual machine. On the left, a list of virtual machines is visible, with 'VM-WS19OpApp' selected. The main area displays the 'Overview' page for this VM, showing its status as 'Stopped (deallocated)' and its location as 'East US'. The 'Essentials' section provides key details like the resource group, subscription ID, and virtual network. The 'Properties' section lists attributes such as the computer name 'VM-WS16OpWeb', operating system 'Windows', and publisher 'MicrosoftWindowsServer'. The 'Networking' section shows the public and private IP addresses.

Data and Encryption

1. Proof of Encryption types for VM (devapp,DevWeb,OpWeb,HRL-App,OPApp, HRL-Web)

vm-ws16devapp-osdisk - Micros x +

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/RG-DEV/providers/Microsoft.Co...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CLAUDACITY1021...)

Home > Virtual machines > vm-ws16devapp | Disks > vm-ws16devapp-osdisk

vm-ws16devapp-osdisk | Encryption

Search

Save Discard Refresh

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type *
Encryption at-rest with a customer-managed key

Disk encryption set *
diskencryptiontheproject123

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template
- Help

VM-WS16DevWeb-osdisk - Micros x +

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/RG-DEV/providers/Microsoft.Co...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CLAUDACITY1021...)

Home > Virtual machines > VM-WS16DevWeb | Disks > VM-WS16DevWeb-osdisk

VM-WS16DevWeb-osdisk | Encryption

Search

Save Discard Refresh

Successfully updated disk
Successfully updated disk 'VM-WS16DevWeb-osdisk'.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type
Encryption at-rest with a customer-managed key

Disk encryption set
diskencryptiontheproject123

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template
- Help

VM-WS16OpWeb-osdisk - Micro x +

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/RG-OPERATIONS/providers/Mic...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CLAUDACITY1021...)

Home > Virtual machines > VM-WS16OpWeb | Disks > VM-WS16OpWeb-osdisk

VM-WS16OpWeb-osdisk | Encryption

Disk

Search Save Discard Refresh

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type
Encryption at-rest with a customer-managed key

Disk encryption set
diskencryptiontheproject123

Successfully updated disk
Successfully updated disk 'VM-WS16OpWeb-osdisk'.

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template
- Help

VM-WS19HRL-App-osdisk - Micro x +

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/RG-HRLEGAL/providers/Micros... UDACITY 1021 (CLAUDACITY1021...)

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CLAUDACITY1021...)

Home > Virtual machines > VM-WS19HRL-App | Disks > VM-WS19HRL-App-osdisk

VM-WS19HRL-App-osdisk | Encryption

Disk

Search Save Discard Refresh

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type
Encryption at-rest with a customer-managed key

Disk encryption set
diskencryptiontheproject123

Successfully updated disk
Successfully updated disk 'VM-WS19HRL-App-osdisk'.

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template
- Help

VM-WS19OpApp-osdisk - Micro x +

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/RG-OPERATIONS/providers/Mic...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud...
UDACITY 1021 (CLAUDACITY1021...)

Home > Virtual machines > VM-WS19OpApp | Disks > VM-WS19OpApp-osdisk

VM-WS19OpApp-osdisk | Encryption

Disk

Search

Save Discard Refresh

Successfully updated disk
Successfully updated disk 'VM-WS19OpApp-osdisk'.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type
Encryption at-rest with a customer-managed key

Disk encryption set
diskencryptiontheproject123

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template
- Help

VM-WS19HRL-Web-osdisk - Micro x +

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/RG-HRLEGAL/providers/Micros...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud...
UDACITY 1021 (CLAUDACITY1021...)

Home > Virtual machines > VM-WS19HRL-Web | Disks > VM-WS19HRL-Web-osdisk

VM-WS19HRL-Web-osdisk | Encryption

Disk

Search

Save Discard Refresh

Successfully updated disk
Successfully updated disk 'VM-WS19HRL-Web-osdisk'.

Azure offers server-side encryption with platform-managed keys by default for managed disks. You may optionally choose to use a customer-managed key. [Learn more](#)

Encryption type
Encryption at-rest with a customer-managed key

Disk encryption set
diskencryptiontheproject123

- Overview
- Activity log
- Access control (IAM)
- Tags
- Settings
 - Configuration
 - Size + performance
 - Encryption
 - Networking
 - Disk Export
 - Properties
 - Locks
- Monitoring
 - Metrics
- Automation
 - Tasks (preview)
 - Export template
- Help

2. Firewalls and virtual networks page

a. Proof of no public access and TLS for SQL servers(prod, dev)

The screenshot shows the Azure portal interface for an SQL server named 'sql-devdata-208323'. The left-hand navigation pane is visible, with 'Networking' selected under the 'Security' category. The main content area displays the 'Public network access' settings. The 'Public network access' section has two radio button options: 'Disable' (which is selected) and 'Selected networks'. Below these options, a blue information box states: 'Only approved private endpoint connections will be accepted by this resource. Any existing firewall rules or virtual network endpoints will be retained, but disabled. Learn more'. At the bottom of the settings pane, there are 'Save' and 'Discard' buttons.

The screenshot shows the Azure portal interface for the same SQL server, but now the 'Private access' tab is selected. The 'Private endpoint connections' section is active, showing a list of connections. At the top of this section, there are buttons for '+ Create a private endpoint', 'Refresh', 'Approve', 'Reject', and 'Remove'. Below these buttons is a search box labeled 'Filter by name...'. The table below is currently empty, with columns for 'Private endpoint', 'Connection name', 'Connection state', and 'Description'.

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG... | Microsoft Azure

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323 | Networking

Create a private endpoint

1 Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * Udacity 1021

Resource group * rg-devdata
[Create new](#)

Instance details

Name * privateendpoint-project

Network Interface Name * privateendpoint-project-nic

Region * East US

< Previous Next: Resource >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG... | Microsoft Azure

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323 | Networking

Create a private endpoint

✓ Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription Udacity 1021 (2c66b487-2f2e-48cd-9374-92db8d0ec2d2)

Resource type Microsoft.Sql/servers

Resource sql-devdata-208323

Target sub-resource * sqlServer

< Previous Next: Virtual Network >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud...
UDACITY 1021 (CLAUDACTY1021...

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323 | Networking >

Create a private endpoint

Basics
 Resource
 Virtual Network
 DNS
 Tags
 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network *

Subnet *

Network policy for private endpoints Disabled (edit)

Private IP configuration

Dynamically allocate IP address
 Statically allocate IP address

Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

+ Create

Application security group

< Previous Next: DNS >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud...
UDACITY 1021 (CLAUDACTY1021...

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323 | Networking >

Create a private endpoint

Basics
 Resource
 Virtual Network
 DNS
 Tags
 Review + create

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone Yes No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-database-win...	Udacity 1021	rg-dev	(new) privatelink.databas...

< Previous Next: Tags >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323 | Networking >

Create a private endpoint

Validation passed

Basics Resource Virtual Network DNS Tags **Review + create**

Basics

Subscription	Udacity 1021
Resource group	rg-devdata
Region	East US
Name	privateendpoint-project
Network Interface Name	privateendpoint-project-nic

Resource

Subscription ID	2c66b487-2f2e-48cd-9374-92db8d0ec2d2 (Udacity 1021)
Link type	Microsoft.Sql/servers
Resource group	rg-devdata
Resource	sql-devdata-208323
Target sub-resource	sqlServer

Virtual Network

Virtual network resource group	rg-dev
Virtual network	Vnet-Dev
Subnet	Vnet-Dev/default (10.2.0.0/24)

Create < Previous Next > Download a template for automation

privateendpoint-project - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourcegroups/rg-devdata/providers/Microsoft...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft.PrivateEndpoint-20220925214743 | Overview >

privateendpoint-project

Private endpoint

Search Delete Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Application security groups
- DNS configuration
- Properties
- Locks

Monitoring

- Insights
- Alerts
- Metrics

Automation

- Tasks (preview)
- Export template

Help

Essentials

Resource group (move)	: rg-devdata	Virtual network/subnet	: Vnet-Dev/default
Location	: East US	Network interface	: privateendpoint-project-nic
Subscription (move)	: Udacity_1021	Private link resource	: sql-devdata-208323
Subscription ID	: 2c66b487-2f2e-48cd-9374-92db8d0ec2d2	Target sub-resource	: sqlServer
Provisioning state	: Succeeded	Connection status	: Approved
Tags (edit)	: Click here to add tags	Request/Response	: Auto-approved

JSON View

sql-devdata-208323 - Microsoft | portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-devdata/providers/Microsoft...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CLAUDACTY1021...)

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323

sql-devdata-208323 | Networking

SQL server

Search

DTU quota

Properties

Locks

Data management

- Backups
- Deleted databases
- Failover groups
- Import/Export history

Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption
- Identity
- Auditing

Intelligent Performance

- Automatic tuning
- Recommendations

Feedback

Public access Private access Connectivity

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following network rules still requires proper authorization to access this resource. [Learn more](#)

Public network access

Disable

Selected networks

Only approved private endpoint connections will be accepted by this resource. Any existing firewall rules or virtual network endpoints will be retained, but disabled. [Learn more](#)

Save Discard

Resolving host...

sql-devdata-208323 - Microsoft | portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-devdata/providers/Microsoft...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CLAUDACTY1021...)

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323

sql-devdata-208323 | Networking

SQL server

Search

DTU quota

Properties

Locks

Data management

- Backups
- Deleted databases
- Failover groups
- Import/Export history

Security

- Networking
- Microsoft Defender for Cloud
- Transparent data encryption
- Identity
- Auditing

Intelligent Performance

- Automatic tuning
- Recommendations

Monitoring

Feedback

Public access **Private access** Connectivity

Private Access

Private endpoints allow access to this resource using a private IP address from a virtual network, effectively bringing the service into your virtual network. [Learn more](#)

Private endpoint connections

+ Create a private endpoint Refresh Approve Reject Remove

Filter by name... Private endpoint == (All)

<input checked="" type="checkbox"/>	Private endpoint	Connection name	Connection state	Description
<input checked="" type="checkbox"/>	privateendpoint-...	privateendpoint-project-769c725...	Approved	Auto-approved

Microsoft Azure portal screenshot showing the Networking configuration page for an Azure SQL server. The page is titled "sql-devdata-208323 | Networking" and includes a left-hand navigation pane with categories like Data management, Security, and Monitoring. The main content area is divided into sections: Outbound networking (Restrictions disabled), Connection Policy (Default selected), and Encryption in transit (Minimum TLS version set to TLS 1.2). Buttons for "Save" and "Discard" are visible at the bottom.

Microsoft Azure portal screenshot showing the Networking configuration page for an Azure SQL server. The page is titled "sql-devdata-208323 | Networking" and includes a left-hand navigation pane with categories like Data management, Security, and Monitoring. The main content area is divided into sections: Outbound networking (Restrictions disabled), Connection Policy (Default selected), and Encryption in transit (Minimum TLS version set to TLS 1.2). Buttons for "Save" and "Discard" are visible at the bottom.

Select a key - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_KeyVault/KeyPickerV2ViewModel/subscriptionsId/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/showSubscriptionDropdown~/true/...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323 | Transparent data encryption >

Select a key

Subscription * Udacity 1021

Key store type Key vault Managed HSM

Key vault * theproject123
[Create new key vault](#)

Key keytheproject123
[Create new key](#)

Version ffb7b2d97eef48f1ab1789fd2c932a9d
[Create new version](#)

Select Cancel

sql-devdata-208323 - Microsoft

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-devdata/providers/Microsoft...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-development-208323 (sql-devdata-208323/DB-development-208323) > sql-devdata-208323

sql-devdata-208323 | Transparent data encryption

SQL server

Search Save Discard Feedback

Settings

- Azure Active Directory
- SQL databases
- SQL elastic pools
- DTU quota
- Properties
- Locks
- Data management
 - Backups
 - Deleted databases
 - Failover groups
 - Import/Export history
- Security
 - Networking
 - Microsoft Defender for Cloud
 - Transparent data encryption
 - Identity
 - Auditing
- Intelligent Performance

Transparent data encryption encrypts your databases, backups, and logs at rest without any changes to your application. To enable encryption, go to each database. [Learn more](#)

Transparent data encryption Service-managed key Customer-managed key

Key selection method Select a key Enter a key identifier

Key * keytheproject123/ffb7b2d97eef48f1ab1789fd2c932a9d
[Change key](#)

Make this key the default TDE protector

Auto-rotate key

Warning: Cutting off access to the key may result in data loss on this server. [Learn more](#)

Info: SQL uses Get, Wrap Key, Unwrap Key permissions to access the selected key vault for TDE. These key vault permissions must be assigned to the managed identity used for TDE (primary user-assigned identity or the system-assigned identity). If needed, we will try granting these permissions on your behalf. [Learn more](#)

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323 | Networking >

Create a private endpoint

1 Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Use private endpoints to privately connect to a service or resource. Your private endpoint must be in the same region as your virtual network, but can be in a different region from the private link resource that you are connecting to. [Learn more](#)

Project details

Subscription * Udacity 1021

Resource group * rg-prod
[Create new](#)

Instance details

Name * privateendpoint-project

Network Interface Name * privateendpoint-project-nic

Region * East US

< Previous Next: Resource >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323 | Networking >

Create a private endpoint

✓ Basics 2 Resource 3 Virtual Network 4 DNS 5 Tags 6 Review + create

Private Link offers options to create private endpoints for different Azure resources, like your private link service, a SQL server, or an Azure storage account. Select which resource you would like to connect to using this private endpoint. [Learn more](#)

Subscription Udacity 1021 (2c66b487-2f2e-48cd-9374-92db8d0ec2d2)

Resource type Microsoft.Sql/servers

Resource sql-proddata-208323

Target sub-resource * sqlServer

< Previous Next: Virtual Network >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323 | Networking >

Create a private endpoint

Basics
 Resource
 Virtual Network
 DNS
 Tags
 Review + create

Networking

To deploy the private endpoint, select a virtual network subnet. [Learn more](#)

Virtual network *

Subnet *

Network policy for private endpoints Disabled (edit)

Private IP configuration

Dynamically allocate IP address
 Statically allocate IP address

Application security group

Configure network security as a natural extension of an application's structure. ASG allows you to group virtual machines and define network security policies based on those groups. You can specify an application security group as the source or destination in an NSG security rule. [Learn more](#)

+ Create

Application security group

< Previous Next: DNS >

Create a private endpoint - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323 | Networking >

Create a private endpoint

Basics
 Resource
 Virtual Network
 DNS
 Tags
 Review + create

Private DNS integration

To connect privately with your private endpoint, you need a DNS record. We recommend that you integrate your private endpoint with a private DNS zone. You can also utilize your own DNS servers or create DNS records using the host files on your virtual machines. [Learn more](#)

Integrate with private DNS zone Yes No

Configuration name	Subscription	Resource group	Private DNS zone
privatelink-database-win...	Udacity 1021	rg-prod	(new) privatelink.databas...

< Previous Next: Tags >

portal.azure.com/#view/Microsoft_Azure_Network/CreatePrivateEndpointBlade/resourceId/%2Fsubscriptions%2F2c66b487-2f2e-48cd-9374-92db8d0ec2d2%2FresourceG...

Microsoft Azure Search resources, services, and docs (G+)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323 | Networking >

Create a private endpoint

Validation passed

Basics Resource Virtual Network DNS Tags **Review + create**

Basics

Subscription	Udacity 1021
Resource group	rg-prod
Region	East US
Name	privateendpoint-project
Network Interface Name	privateendpoint-project-nic

Resource

Subscription ID	2c66b487-2f2e-48cd-9374-92db8d0ec2d2 (Udacity 1021)
Link type	Microsoft.Sql/servers
Resource group	rg-data
Resource	sql-proddata-208323
Target sub-resource	sqlServer

Virtual Network

Virtual network resource group	rg-prod
Virtual network	VNet-prod
Subnet	VNet-prod/Operations (10.1.1.0/24)

Create < Previous Next > Download a template for automation

privateendpoint2-project - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourcegroups/rg-prod/providers/Microsoft.Ne...

Home > Microsoft.PrivateEndpoint-20220925221418 | Overview >

privateendpoint2-project

Private endpoint

Search Delete Refresh

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Application security groups
- DNS configuration
- Properties
- Locks

Monitoring

- Insights
- Alerts
- Metrics

Automation

- Tasks (preview)
- Export template

Help

Essentials

Resource group (move) : [rg-prod](#)

Location : East US

Subscription (move) : [Udacity 1021](#)

Subscription ID : 2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Provisioning state : Succeeded

Tags (edit) : [Click here to add tags](#)

Virtual network/subnet : [VNet-prod/Operations](#)

Network interface : [privateendpoint2-project-nic](#)

Private link resource : [sql-proddata-208323](#)

Target sub-resource : sqlServer

Connection status : Approved

Request/Response : Auto-approved

JSON View

sql-proddata-208323 - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-data/providers/Microsoft.Sql/...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CL4UDACTY1021...)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323

sql-proddata-208323 | Networking

SQL server

Search

- SQL databases
- SQL elastic pools
- DTU quota
- Properties
- Locks
- Data management
 - Backups
 - Deleted databases
 - Failover groups
 - Import/Export history
- Security
 - Networking
 - Microsoft Defender for Cloud
 - Transparent data encryption
 - Identity
 - Auditing
- Intelligent Performance
 - Automatic tuning

Feedback

Public access Private access Connectivity

Public network access

Public Endpoints allow access to this resource through the internet using a public IP address. An application or resource that is granted access with the following network rules still requires proper authorization to access this resource. [Learn more](#)

Public network access

Disable

Selected networks

Only approved private endpoint connections will be accepted by this resource. Any existing firewall rules or virtual network endpoints will be retained, but disabled. [Learn more](#)

Save Discard

sql-proddata-208323 - Microsoft Azure

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-data/providers/Microsoft.Sql/...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@cl4ud... UDACITY 1021 (CL4UDACTY1021...)

Home > SQL databases > DB-operations-208323 (sql-proddata-208323/DB-operations-208323) > sql-proddata-208323

sql-proddata-208323 | Networking

SQL server

Search

- SQL databases
- SQL elastic pools
- DTU quota
- Properties
- Locks
- Data management
 - Backups
 - Deleted databases
 - Failover groups
 - Import/Export history
- Security
 - Networking
 - Microsoft Defender for Cloud
 - Transparent data encryption
 - Identity
 - Auditing
- Intelligent Performance
 - Automatic tuning

Feedback

Public access **Private access** Connectivity

Private Access

Private endpoints allow access to this resource using a private IP address from a virtual network, effectively bringing the service into your virtual network. [Learn more](#)

Private endpoint connections

+ Create a private endpoint Refresh Approve Reject Remove

Filter by name... Private endpoint == (All)

<input type="checkbox"/>	Private endpoint	Connection name	Connection state	Description
<input checked="" type="checkbox"/>	privateendpoint2...	privateendpoint2-project-b73b3...	Approved	Auto-approved
<input type="checkbox"/>	privateendpoint...	privateendpoint-project-9cac454...	Approved	Auto-approved

Microsoft Azure portal showing the Networking configuration page for the SQL server 'sql-proddata-208323'. The page is under the 'Connectivity' tab. The 'Outbound networking' section shows 'Restrictions disabled'. The 'Connection Policy' section has three options: 'Default' (selected), 'Proxy', and 'Redirect'. The 'Encryption in transit' section shows 'Minimum TLS version' set to 'TLS 1.2'. There are 'Save' and 'Discard' buttons at the bottom.

Microsoft Azure portal showing the Networking configuration page for the SQL server 'sql-proddata-208323'. The page is under the 'Connectivity' tab. A notification bubble in the top right corner states: 'Successfully updated server minimum TLS version. Successfully updated minimum TLS version for server sql-proddata-208323'. The 'Outbound networking' section shows 'Restrictions disabled'. The 'Connection Policy' section has three options: 'Default' (selected), 'Proxy', and 'Redirect'. The 'Encryption in transit' section shows 'Minimum TLS version' set to 'TLS 1.2'. There are 'Save' and 'Discard' buttons at the bottom.

3. Proof of Azure Defender SQL server enabled(prod, dev)

The screenshot shows the Microsoft Defender for Cloud interface for a development SQL server named 'sql-devdata-208323'. The page title is 'Microsoft Defender for Cloud'. A notification in the top right corner states: 'Successfully enabled Azure Defender for SQL. Successfully enabled Azure Defender for SQL on server 'sql-devdata-208323''. The main content area displays the following metrics: 8 Recommendations (with a red exclamation mark icon), 0 Security alerts (with a blue shield icon), and Findings (with a green checkmark icon). The Enablement Status is 'Enabled at the subscription-level'. Below these metrics, there is a 'Recommendations' section with a description: 'Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.' A table lists the following recommendations:

Description	Severity
SQL servers should have an Azure Active Directory administrator provisioned	High
Auditing on SQL server should be enabled	Low
Private endpoint connections on Azure SQL Database should be enabled	Medium
Microsoft Defender for SQL should be enabled for unprotected Azure SQL servers	High
Public network access on Azure SQL Database should be disabled	Medium

A link 'View additional recommendations in Defender for Cloud >' is provided at the bottom of the table.

The screenshot shows the Microsoft Defender for Cloud interface for a production SQL server named 'sql-proddata-208323'. The page title is 'Microsoft Defender for Cloud'. A notification in the top right corner states: 'Successfully enabled Azure Defender for SQL. Successfully enabled Azure Defender for SQL on server 'sql-proddata-208323''. The main content area displays the following metrics: 8 Recommendations (with a red exclamation mark icon), 0 Security alerts (with a blue shield icon), and Findings (with a green checkmark icon). The Enablement Status is 'Enabled at the subscription-level'. Below these metrics, there is a 'Recommendations' section with a description: 'Defender for Cloud continuously monitors the configuration of your SQL Servers to identify potential security vulnerabilities and recommends actions to mitigate them.' A table lists the following recommendations:

Description	Severity
SQL servers should have an Azure Active Directory administrator provisioned	High
Vulnerability Assessment settings for SQL server should contain an email address to receive scan reports	Low
SQL servers should use customer-managed keys to encrypt data at rest	Low
Auditing on SQL server should be enabled	Low
Private endpoint connections on Azure SQL Database should be enabled	Medium

A link 'View additional recommendations in Defender for Cloud >' is provided at the bottom of the table.

4. Proof of Azure AD authentication for SQL enabled(prod, dev)

The image displays two screenshots of the Microsoft Azure portal, illustrating the configuration of Azure Active Directory (AD) authentication for SQL servers. Both screenshots show the 'Azure Active Directory' settings page for a specific SQL server.

Top Screenshot: sql-proddata-208323

- Page Title:** sql-proddata-208323 | Azure Active Directory
- Admin name:** Seth@cl4udacity1021.onmicrosoft.com (Admin Object/App ID: 2ac7cb66-4352-4c67-8ac1-4b7dfff7142b)
- Azure Active Directory authentication only:** Only Azure Active Directory will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users.
- Support only Azure Active Directory authentication for this server:**

Bottom Screenshot: sql-devdata-208323

- Page Title:** sql-devdata-208323 | Azure Active Directory
- Admin name:** Seth@cl4udacity1021.onmicrosoft.com (Admin Object/App ID: 2ac7cb66-4352-4c67-8ac1-4b7dfff7142b)
- Azure Active Directory authentication only:** Only Azure Active Directory will be used to authenticate to the server. SQL authentication will be disabled, including SQL Server administrators and users.
- Support only Azure Active Directory authentication for this server:**

Both screenshots include a notification panel on the right side with the following messages:

- Enabled Azure Active Directory authentication only:** Enabled Azure Active Directory authentication only for serverName: sql-proddata-208323
- Set the Azure AD admin:** Set the Azure Active Directory admin for serverName: sql-proddata-208323

Cloud Protection

1. Proof of IaaS Antimalware enabled (devapp, DevWeb, OpApp, HRL-Web, HRL-App, OpWeb)

The screenshot shows the Azure portal interface for the resource 'vm-ws16devapp/iaaSAntimalware'. The breadcrumb trail is: Home > microsoft.antimalware-windows-20220925224932 | Overview >. The resource name is 'vm-ws16devapp/iaaSAntimalware' with the provider 'microsoft.compute/virtualmachines/extensions'. The left-hand navigation menu includes Overview, Activity log, Access control (IAM), Settings (Locks), Automation (Tasks, Export template), and Help (New Support Request). The main content area is divided into three sections: Essentials, Properties, and Instance view. The Essentials section shows the resource group as 'rg-dev', subscription as 'Udacity_1021', and subscription ID as '2c66b487-2f2e-48cd-9374-92db8d0ec2d2'. The Properties section lists: Force update tag (---), Publisher (Microsoft.Azure.Security), Type (IaaSAntimalware), Type handler version (1.3), Auto upgrade minor ver... (true), Enable automatic upgra... (---), Settings (View value as JSON), Protected settings (---), Provisioning state (Succeeded), and Suppress failures (---). The Instance view section shows: Name (---), Type (---), Type handler version (---), Substatuses (---), and Statuses (---).

The screenshot shows the Azure portal interface for the resource 'VM-WS16DevWeb/iaaSAntimalware'. The breadcrumb trail is: Home > microsoft.antimalware-windows-20220925225655 | Overview >. The resource name is 'VM-WS16DevWeb/iaaSAntimalware' with the provider 'microsoft.compute/virtualmachines/extensions'. The left-hand navigation menu is identical to the first screenshot. The main content area is divided into three sections: Essentials, Properties, and Instance view. The Essentials section shows the resource group as 'rg-dev', subscription as 'Udacity_1021', and subscription ID as '2c66b487-2f2e-48cd-9374-92db8d0ec2d2'. The Properties section lists: Force update tag (---), Publisher (Microsoft.Azure.Security), Type (IaaSAntimalware), Type handler version (1.3), Auto upgrade minor ver... (true), Enable automatic upgra... (---), Settings (View value as JSON), Protected settings (---), Provisioning state (Succeeded), and Suppress failures (---). The Instance view section shows: Name (---), Type (---), Type handler version (---), Substatuses (---), and Statuses (---).

Home > microsoft.antimalware-windows-20220925225900 | Overview >

VM-WS16OpWeb/laaSantimalware

Search Refresh Delete

- Overview
- Activity log
- Access control (IAM)
- Settings
 - Locks
- Automation
 - Tasks (preview)
 - Export template
- Help
 - New Support Request

Essentials

Resource group (move) : [rg-operations](#)
Subscription (move) : [Udacity_1021](#)
Subscription ID : 2c66b487-2f2e-48cd-9374-92db8d0ec2d2
Tags (edit) : [Click here to add tags](#)

Resource id : [/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups...](#)
Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag ○ ---
Publisher ○ Microsoft.Azure.Security
Type ○ IaaSantimalware
Type handler version ○ 1.3
Auto upgrade minor ver... ○ true
Enable automatic upgra... ○ ---
Settings ○ [View value as JSON](#)
Protected settings ○ ---
Provisioning state ○ Succeeded
Suppress failures ○ ---

Instance view

Name ○ ---
Type ○ ---
Type handler version ○ ---
Substatuses ○ ---
Statuses ○ ---

Home > microsoft.antimalware-windows-20220925230107 | Overview >

VM-WS19HRL-App/laaSantimalware

Search Refresh Delete

- Overview
- Activity log
- Access control (IAM)
- Settings
 - Locks
- Automation
 - Tasks (preview)
 - Export template
- Help
 - New Support Request

Essentials

Resource group (move) : [rg-hrlegal](#)
Subscription (move) : [Udacity_1021](#)
Subscription ID : 2c66b487-2f2e-48cd-9374-92db8d0ec2d2
Tags (edit) : [Click here to add tags](#)

Resource id : [/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups...](#)
Type : Microsoft.Compute/virtualMachines/extensions

Properties

Force update tag ○ ---
Publisher ○ Microsoft.Azure.Security
Type ○ IaaSantimalware
Type handler version ○ 1.3
Auto upgrade minor ver... ○ true
Enable automatic upgra... ○ ---
Settings ○ [View value as JSON](#)
Protected settings ○ ---
Provisioning state ○ Succeeded
Suppress failures ○ ---

Instance view

Name ○ ---
Type ○ ---
Type handler version ○ ---
Substatuses ○ ---
Statuses ○ ---

VM-WS19HRL-Web/laaSAntimalware

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-hrlegal/providers/Microsoft...

Microsoft Azure Search resources, services, and docs (G+)

Home > microsoft.antimalware-windows-20220925230259 | Overview >

VM-WS19HRL-Web/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search Refresh Delete

Overview

- Activity log
- Access control (IAM)

Settings

- Locks

Automation

- Tasks (preview)
- Export template

Help

- New Support Request

Essentials

Resource group (move) : [rg-hrlegal](#)

Subscription (move) : [Udacity_1021](#)

Subscription ID : 2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Tags (edit) : [Click here to add tags](#)

Resource id : [/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups...](#)

Type : Microsoft.Compute/virtualMachines/extensions

JSON View

Properties

- Force update tag : ---
- Publisher : Microsoft.Azure.Security
- Type : laaSAntimalware
- Type handler version : 1.3
- Auto upgrade minor ver... : true
- Enable automatic upgra... : ---
- Settings : [View value as JSON](#)
- Protected settings : ---
- Provisioning state : Succeeded
- Suppress failures : ---

Instance view

- Name : ---
- Type : ---
- Type handler version : ---
- Substatuses : ---
- Statuses : ---

VM-WS19OpApp/laaSAntimalware

portal.azure.com/#@cl4udacity1021.onmicrosoft.com/resource/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups/rg-operations/providers/Micros...

Microsoft Azure Search resources, services, and docs (G+)

Home > microsoft.antimalware-windows-20220925230549 | Overview >

VM-WS19OpApp/laaSAntimalware

microsoft.compute/virtualmachines/extensions

Search Refresh Delete

Overview

- Activity log
- Access control (IAM)

Settings

- Locks

Automation

- Tasks (preview)
- Export template

Help

- New Support Request

Essentials

Resource group (move) : [rg-operations](#)

Subscription (move) : [Udacity_1021](#)

Subscription ID : 2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Tags (edit) : [Click here to add tags](#)

Resource id : [/subscriptions/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroups...](#)

Type : Microsoft.Compute/virtualMachines/extensions

JSON View

Properties

- Force update tag : ---
- Publisher : Microsoft.Azure.Security
- Type : laaSAntimalware
- Type handler version : 1.3
- Auto upgrade minor ver... : true
- Enable automatic upgra... : ---
- Settings : [View value as JSON](#)
- Protected settings : ---
- Provisioning state : Succeeded
- Suppress failures : ---

Instance view

- Name : ---
- Type : ---
- Type handler version : ---
- Substatuses : ---
- Statuses : ---

2. Recommendations

The screenshot displays the Microsoft Defender for Cloud Recommendations interface. At the top, the secure score is 43%. Below this, there are sections for Active items (Controls: 3/14, Recommendations: 0/0), Resource health (Unhealthy: 0, Healthy: 0, Not applicable: 18), and Governance (preview) (Overdue recommendations: 0/0, Unassigned recommendations: 0/0). A table of recommendations is shown below, sorted by potential score increase. The table has columns for Name, Max score, Current score, Potential score increase, Status, Unhealthy resources, and Insights.

Name	Max score	Current score	Potential score increase	Status	Unhealthy resources	Insights
Enable encryption at rest	4	4.00		Completed	0 of 8 resources	
Remediate security configurations	4	0.00	+ 44%	Unassigned	2 of 8 resources	
Enable auditing and logging	1	0.00	+ 11%	Unassigned	5 of 5 resources	
Remediate vulnerabilities	Not scored	Not scored		Completed	0 of 6 resources	
Enable endpoint protection	Not scored	Not scored		Completed	0 of 6 resources	

As listed in the screenshot above, there are three scored recommendation which should be resolved.

1- Enable encryption at rest: virtual machines and SQL databases must be encrypted in a secured environment.

2- Remediate security configurations: log analytics agent should be installed on virtual machines, machines should be configured securely, vulnerabilities in security configuration on your windows machines should be remediated, and SQL servers should have vulnerability assessment configured.

3- Enable auditing and logging: auditing on SQL server should be enabled, and diagnostic logs in key vault should be enabled.

Notes:

- It's a good practice to sort the recommendations by potential score increase.
- For every recommendation it can basically give me some ideas of how I can resolve the issue.
- For some issues the security center gives me the opportunity to resolve it right through itself.

Monitoring

1. Proof of Azure SQL auditing with Log analytics (devdata,proddata)

The screenshot displays the Microsoft Azure portal interface for configuring Azure SQL Auditing. The main content area shows the 'Azure SQL Auditing' settings for the database 'DB-development-208323 (sql-devdata-208323/DB-development-208323)'. The 'Enable Azure SQL Auditing' toggle is turned on. Under 'Audit log destination (choose at least one):', the 'Log Analytics' checkbox is checked, and the 'Storage' checkbox is unchecked. The 'Subscription' dropdown is set to 'Udacity 1021' and the 'Log Analytics' dropdown is set to 'sentinel-project(eastus)'. A 'Success' notification box is overlaid on the right, stating 'Successfully saved Auditing settings.' and 'Successfully saved database Auditing settings'. The left sidebar shows the navigation menu with 'Auditing' selected under the 'Security' section. The top navigation bar includes the Microsoft Azure logo and a search bar.

The screenshot shows the Azure portal interface for configuring SQL Auditing. On the left, a navigation pane lists various settings like Compute + storage, Connection strings, Properties, Locks, Data management, Integrations, Security, Auditing, Ledger, Data Discovery & Classification, Dynamic Data Masking, Microsoft Defender for Cloud, and Transparent data encryption. The 'Auditing' section is selected. The main content area shows the 'Azure SQL Auditing' configuration. A toggle switch for 'Enable Azure SQL Auditing' is turned on. Under 'Audit log destination (choose at least one)', the 'Log Analytics' checkbox is checked. Below this, the 'Subscription' is set to 'Udacity 1021' and 'Log Analytics' is set to 'sentinel-project(eastus)'. A 'Success' message at the top right states: 'Successfully saved database Auditing settings. Successfully saved Auditing settings for database: DB-operations-208323. View dashboard in Log Analytics workspace summary'.

2. Proof of Sentinel connectors (2+)

The screenshot shows the 'Create Log Analytics workspace' page in the Azure portal. At the top, a green banner indicates 'Validation passed'. Below this, there are tabs for 'Basics', 'Tags', and 'Review + Create'. The 'Basics' tab is active, showing the following details:

Subscription	Udacity 1021
Resource group	rg-core
Name	sentinel-project
Region	East US
Pricing tier	Pay-as-you-go (Per GB 2018)

Below the table, there is a note: 'The cost of your workspace depends on the volume of data ingested and how long it is retained. Regional pricing details are available on the [Azure Monitor pricing page](#). You can change to a different pricing tier after the workspace is created. [Learn more about Log Analytics pricing models.](#)' At the bottom, there are buttons for 'Create', 'Previous', and 'Download a template for automation'.

portalazure.com/#view/Microsoft_Azure_Security_Insights/OnboardingBlade/_provisioningContext~/~/%7B%22initialValues%3A%7B%22subscriptionIds%3A%5B%5D%2C%22resou...


Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace

+ Create a new workspace Refresh

Microsoft Sentinel offers a 31-day free trial. See [Microsoft Sentinel pricing](#) for more details.

Filter by name...



No workspaces found

Create a new workspace

Add Cancel

Microsoft Sentinel - Microsoft A...

portalazure.com/#view/Microsoft_Azure_Security_Insights/MainMenuBlade/~/_/DataConnectors/subscriptionId/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/resourceGroup/...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel

Microsoft Sentinel | Data connectors

Selected workspace: 'sentinel-project'

Search Refresh Guides & Feedback

124 Connectors 0 Connected More content at Content hub

Search by name or provider Providers: All Data Types: All Status: All

Status	Connector name ↑
	Aruba ClearPass (Preview) Aruba Networks
	Atlassian Confluence Audit (Preview) Atlassian
	Atlassian Jira Audit (Preview) Atlassian
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft
	Azure Activity Microsoft
	Azure DDoS Protection Microsoft

Azure Active Directory Identity Protection

Disconnected Status Microsoft Provider Last Log Received

Description

Azure Active Directory Identity Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft's experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. Integrate Microsoft Azure Active Directory Identity Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.

[Get Azure Active Directory Premium P1/P2 >](#)

Last data received

..

Related content

Open connector page

Microsoft Azure portal showing the configuration page for Azure Active Directory Identity Protection. The page is titled "Azure Active Directory Identity Protection" and includes a navigation breadcrumb: Home > Microsoft Sentinel > Add Microsoft Sentinel to a workspace > Microsoft Sentinel | Data connectors > Azure Active Directory Identity Protection.

The left sidebar shows the connector details:

- Connected Status:** Microsoft Provider, Last Log Received: --
- Description:** Azure Active Directory Identity Protection provides a consolidated view at risk users, risk events and vulnerabilities, with the ability to remediate risk immediately, and set policies to auto-remediate future events. The service is built on Microsoft's experience protecting consumer identities and gains tremendous accuracy from the signal from over 13 billion logins a day. Integrate Microsoft Azure Active Directory Identity Protection alerts with Microsoft Sentinel to view dashboards, create custom alerts, and improve investigation.
- Get Azure Active Directory Premium P1/P2 >**
- Last data received:** --
- Related content:** 0 Workbooks, 2 Queries, 3 Analytics rules templates
- Data received:** A line chart showing data received over time, with a "Go to log analytics" link.

The main content area is divided into sections:

- Instructions:**
 - Prerequisites:** To integrate with Azure Active Directory Identity Protection make sure you have:
 - ✓ **Workspace:** read and write permissions.
 - ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
 - ✓ **License:** Azure AD Premium P2
 - Configuration:** Azure Active Directory Identity Protection alerts to Microsoft Sentinel. Connect Azure Active Directory Identity Protection to Microsoft Sentinel. The alerts are sent to this Microsoft Sentinel workspace. A "Disconnect" button is visible.

The same Microsoft Azure portal page is shown, but with a notification banner at the top right: "Microsoft incident creation rule added successfully".

The configuration section has been updated:

- Prerequisites:**
 - ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.
 - ✓ **License:** Azure AD Premium P2
- Configuration:** The text remains the same, but the "Disconnect" button is now disabled.
- Create incidents - Recommended!** A new section with a briefcase icon, stating "Create incidents automatically from all alerts generated in this connected service." with an "Enabled" button.

Home > Microsoft Sentinel > Microsoft Sentinel

Microsoft Sentinel

Udacity 1021 (cl4udacity1021.onmicrosoft.com)

+ Create Manage view

Filter for any field...

Name ↑

sentinel-project

Microsoft Sentinel | Data connectors

Selected workspace: 'sentinel-project'

Search

Refresh Guides & Feedback

124 Connectors 1 Connected More content at Content hub

azure active Providers: All Data Types: All

Status	Connector name ↑
	Azure Active Directory Microsoft
	Azure Active Directory Identity Protection Microsoft

Azure Active Directory

Disconnect... Microsoft Last Log Rec...

Description
Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received
--

Related content

Open connector page

Azure Active Directory - Microsoft | Security alerts - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Security_Insights/DataConnectorBlade/dataConnectorId/AzureActiveDirectory/initialConnectorTab~/0/subscriptionId/2c66b487-...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

Azure Active Directory

Azure Active Directory

Not connected Microsoft Provider Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received

Related content

8 Workbooks 2 Queries 99 Analytics rules templates

Data received Go to log analytics

100
80
60
40
20
0

Instructions Next steps

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Diagnostic Settings:** read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel

Select Azure Active Directory log types:

Sign-In Logs

i In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

Audit Logs

Non-Interactive User Sign-In Log (Preview)

Azure Active Directory - Microsoft | Security alerts - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Security_Insights/DataConnectorBlade/dataConnectorId/AzureActiveDirectory/initialConnectorTab~/0/subscriptionId/2c66b487-2f2e-...

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Sentinel > Microsoft Sentinel | Data connectors >

Azure Active Directory

Azure Active Directory

Connected Microsoft Provider 13 minutes ago Last Log Received

Description

Gain insights into Azure Active Directory by connecting Audit and Sign-in logs to Microsoft Sentinel to gather insights around Azure Active Directory scenarios. You can learn about app usage, conditional access policies, legacy auth relate details using our Sign-in logs. You can get information on your Self Service Password Reset (SSPR) usage, Azure Active Directory Management activities like user, group, role, app management using our Audit logs table.

Last data received

09/26/22, 01:31 AM

Related content

8 Workbooks 2 Queries 99 Analytics rules templates

Data received Go to log analytics

5	AADNonInt...
4	AADService...
3	AADManag...
2	
1	
0	

Instructions Next steps

Prerequisites

To integrate with Azure Active Directory make sure you have:

- ✓ **Workspace:** read and write permissions.
- ✓ **Diagnostic Settings:** read and write permissions to AAD diagnostic settings.
- ✓ **Tenant Permissions:** 'Global Administrator' or 'Security Administrator' on the workspace's tenant.

Configuration

Connect Azure Active Directory logs to Microsoft Sentinel

Select Azure Active Directory log types:

Sign-In Logs

i In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

Audit Logs

Non-Interactive User Sign-In Log (Preview)

Compliance

1. Proof of NIST SP 800-53 rev4 policy added

Settings - Microsoft Azure | Security - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/policy/subscriptionId/2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Microsoft Azure Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Regulatory compliance > Environment settings > Settings

Settings | Security policy

Udacity 1021

Search

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export

Policy settings

- Security policy
- Governance rules (preview)

Security policy on: Udacity 1021

initiatives enabled on this subscription

Default initiative

No existing Policy assignments

[Assign policy](#)

Industry & regulatory standards

Compliance initiatives shown in the **Regulatory compliance dashboard**.

Azure Security Benchmark	Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable	ⓘ
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable	ⓘ
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set	Out of the box	Deprecated	ⓘ

Settings - Microsoft Azure | Security - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Security/PolicyMenuBlade/~/policy/subscriptionId/2c66b487-2f2e-48cd-9374-92db8d0ec2d2

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@clAud... UDACITY 1021 (CLAUDACTY1021...)

Home > Microsoft Defender for Cloud | Regulatory compliance > Environment settings > Settings

Settings | Security policy

Udacity 1021

Search

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export

Policy settings

- Security policy
- Governance rules (preview)

Name	Description	Source	Actions
PCI DSS 3.2.1	Track PCI-DSS v3.2.1-2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Deprecated
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable
Azure CIS 1.3.0	Track Azure CIS 1.3.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete

[Add more standards](#)

Your custom initiatives

Custom initiatives generate custom recommendations in the **Recommendations** page.

[Add a custom initiative](#)

Add regulatory compliance stan... | Security - Microsoft Azure

portal.azure.com/#view/Microsoft_Azure_Security/AddPolicyPackagesBlade/isFree~/false/scopeld/2c66b487-2f2e-48cd-9374-92db8d0ec2d2/scopeType~/0/policyPackag...

Microsoft Azure Search resources, services, and docs (G+)

odl_user_208323@clAud... UDACITY 1021 (CLAUDACTY1021...)

Home > Microsoft Defender for Cloud | Regulatory compliance > Environment settings > Settings | Security policy >

Add regulatory compliance standards

Click **Add** on the standards that you want to add to the regulatory compliance dashboard and then assign it to the subscription. After completing the assignment, the custom policies will be available in the **Regulatory compliance** dashboard.

Search to filter items...

Name	Description	Actions
NIST SP 800-53 R4	Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
NIST SP 800 171 R2	Track NIST SP 800 171 R2 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
UKO and UK NHS	Track UK OFFICIAL and UK NHS controls in the Compliance Dashboard, based on a recommended set of policies and assessm...	Add
Canada Federal PBMM	Track Canada Federal PBMM controls in the Compliance Dashboard, based on a recommended set of policies and assessmen...	Add
Azure CIS 1.1.0	Track Azure CIS 1.1.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
HIPAA HITRUST	Track HIPAA/HITRUST controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
SWIFT CSP CSCF v2020	Track SWIFT CSP CSCF v2020 controls in the Compliance Dashboard, based on a recommended set of policies and assessmen...	Add
ISO 27001:2013	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
New Zealand ISM Restricted	Track New Zealand ISM Restricted controls in the Compliance Dashboard, based on a recommended set of policies and asses...	Add
CMMC Level 3	Track CMMC Level 3 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
NIST SP 800-53 R5	Track NIST SP 800-53 R5 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
FedRAMP H	Track FedRAMP H controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
FedRAMP M	Track FedRAMP M controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
RMIT Malaysia	Track RMIT Malaysia controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Add
Australian Government ISM PROTECTED	Track Australian Government ISM PROTECTED controls in the Compliance Dashboard, based on a recommended set of polici...	Add
New Zealand ISM Restricted v3.5	Track New Zealand ISM Restricted v3.5 controls in the Compliance Dashboard, based on a recommended set of policies and ...	Add

Microsoft Azure portal. Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Regulatory compliance > Environment settings > Settings | Security policy > Add regulatory compliance standards >

NIST SP 800-53 Rev. 4

Assign initiative

Basics Parameters Remediation Non-compliance messages Review + create

Scope
 Scope [Learn more about setting the scope](#) *

Udacity 1021

Exclusions
 Optionally select resources to exclude from the policy assignment.

Basics
 Initiative definition
 NIST SP 800-53 Rev. 4

Assignment name * ⓘ
 NIST SP 800-53 Rev. 4

Description

Policy enforcement ⓘ
 Enabled Disabled

[Review + create](#) [Cancel](#) [Previous](#) [Next](#)

Microsoft Azure portal. Search resources, services, and docs (G+)

Home > Microsoft Defender for Cloud | Regulatory compliance > Environment settings > Settings | Security policy > Add regulatory compliance standards >

NIST SP 800-53 Rev. 4

Assign initiative

Basics Parameters Remediation Non-compliance messages Review + create

Basics

Scope	Udacity 1021
Exclusions	--
Policy definition	NIST SP 800-53 Rev. 4
Assignment name	NIST SP 800-53 Rev. 4
Description	--
Policy enforcement	Enabled
Assigned by	ODL_User 208323

Parameters

No parameter changes detected.

Remediation

Create managed identity	Yes
System assigned identity location	eastus
Create a remediation task	No

Non-compliance messages

No non-compliance messages associated with this assignment.

[Create](#) [Cancel](#) [Previous](#) [Next](#)

Settings | Security policy

- Settings
- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Policy settings
 - Security policy
 - Governance rules (preview)

PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Deprecated
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	Enable
Azure CIS 1.3.0	Track Azure CIS 1.3.0 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete
NIST SP 800-53 R4	Track NIST SP 800-53 R4 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Manually added	Delete

[Add more standards](#)

Your custom initiatives

Custom initiatives generate custom recommendations in the **Recommendations** page.

- Policy added**
NIST SP 800-53 R4 policy initiative was assigned on Udacity 1021 Subscription successfully. Please note that it could take up to an hour until the changes in the regulatory compliance dashboard will take effect.
- Role Assignments creation succeeded**
All role assignments were created successfully.
- Creating initiative assignment succeeded**
Creating initiative assignment 'NIST SP 800-53 Rev. 4' in 'Udacity 1021' was successful. Please note that the assignment takes around 30 minutes to take effect.