

12. Cisco AnyConnect, Azure SAML2实战



教主技术进化论 2022

教主VIP, 聊点高级的!

Azure AD Connect





创建管理员

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

Home > Default Directory > 1

Users | All users ...

Default Directory - Azure Active Directory

3 + New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user Columns Got feedback?

2 All users Deleted users Password reset User settings Diagnose and solve problems

Activity

Sign-in logs Audit logs Bulk operation results

Troubleshooting + Support

New support request

Search users Add filters

1 user found

Name	User principal na...↑↓	User type	Directory synced	Account enabled	Identity issuer	Company name	Creation type
<input type="checkbox"/> 秦柯 秦柯	collinsctk_qytang.co...	Member	No	Yes	MicrosoftAccount		



创建管理员

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

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Users >

New user

Default Directory

Got feedback?

Create user
Create a new user in your organization. This user will have a user name like alice@qytang.com.
[I want to create users in bulk](#)

Invite user
Invite a new guest user to collaborate with your organization. The user will be emailed an invitation they can accept in order to begin collaborating.
[I want to invite guest users in bulk](#)

[Help me decide](#)

Identity

User name * @

The domain name I need isn't shown here

Name *

First name

Last name

Password

Auto-generate password

Let me create the password

Initial password *

Groups and roles

Groups 0 groups selected

[Create](#)



创建管理员

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

Home > Default Directory > Users >

New user

Default Directory

Got feedback?

Last name

Password

Auto-generate password

Let me create the password

Initial password *

Groups and roles

Groups 0 groups selected

Roles **Global administrator** 1

Settings

Block sign in Yes **No**

Usage location

Job info

Job title

Department

Company name

Manager No manager selected

Create 2



创建管理员

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

Home > Default Directory >

Users | All users

Default Directory - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user Columns Got feedback?

Search users Add filters

2 users found

	Name	User principal na...↑↓	User type	Directory synced	Account enabled	Identity issuer	Company name	Creation type
<input type="checkbox"/>	AD adadmin	adadmin@qytang.com	Member	No	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/>	秦柯 秦柯	collinsctk_qytang.co...	Member	No	Yes	MicrosoftAccount		

Activity

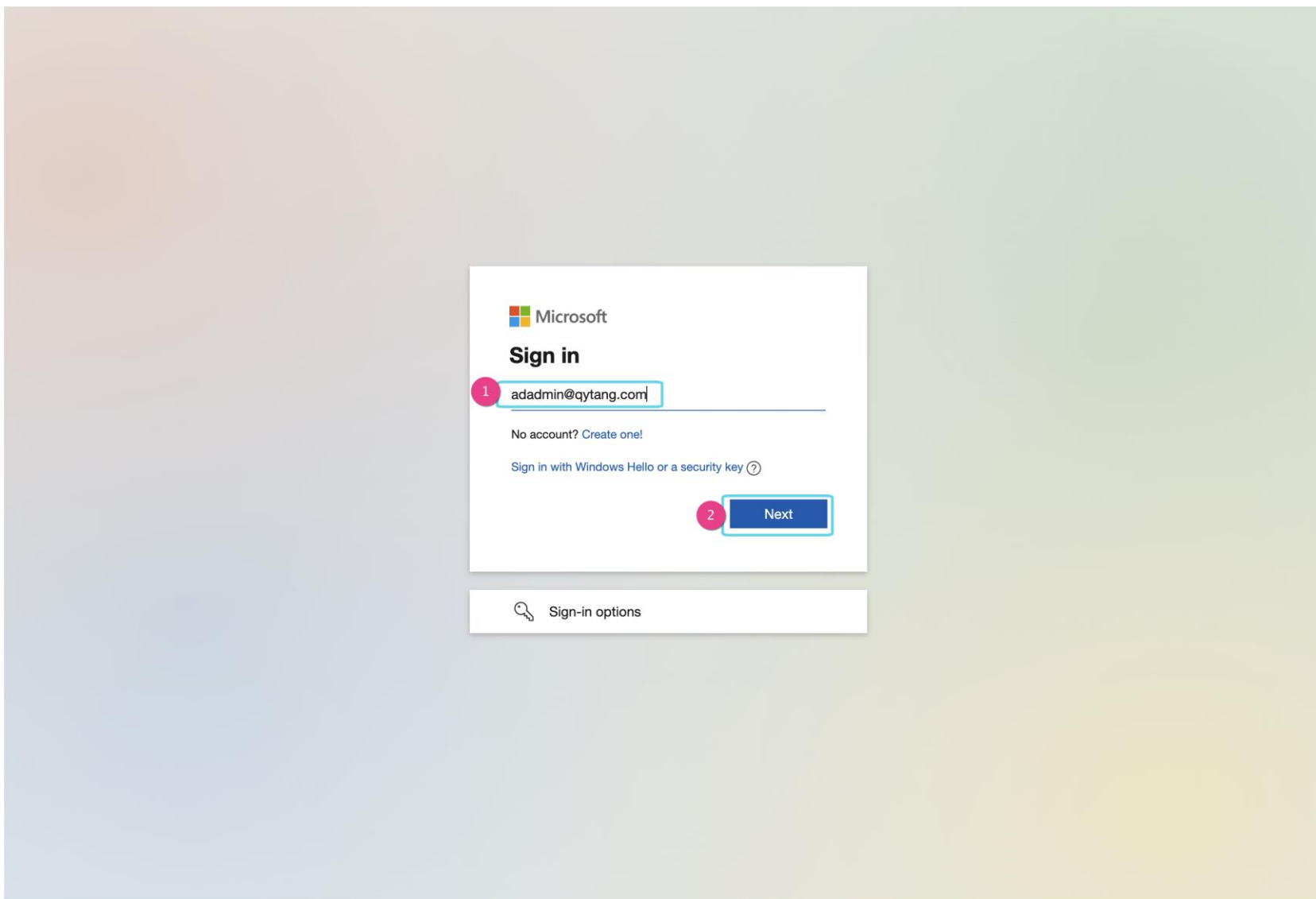
- Sign-in logs
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request

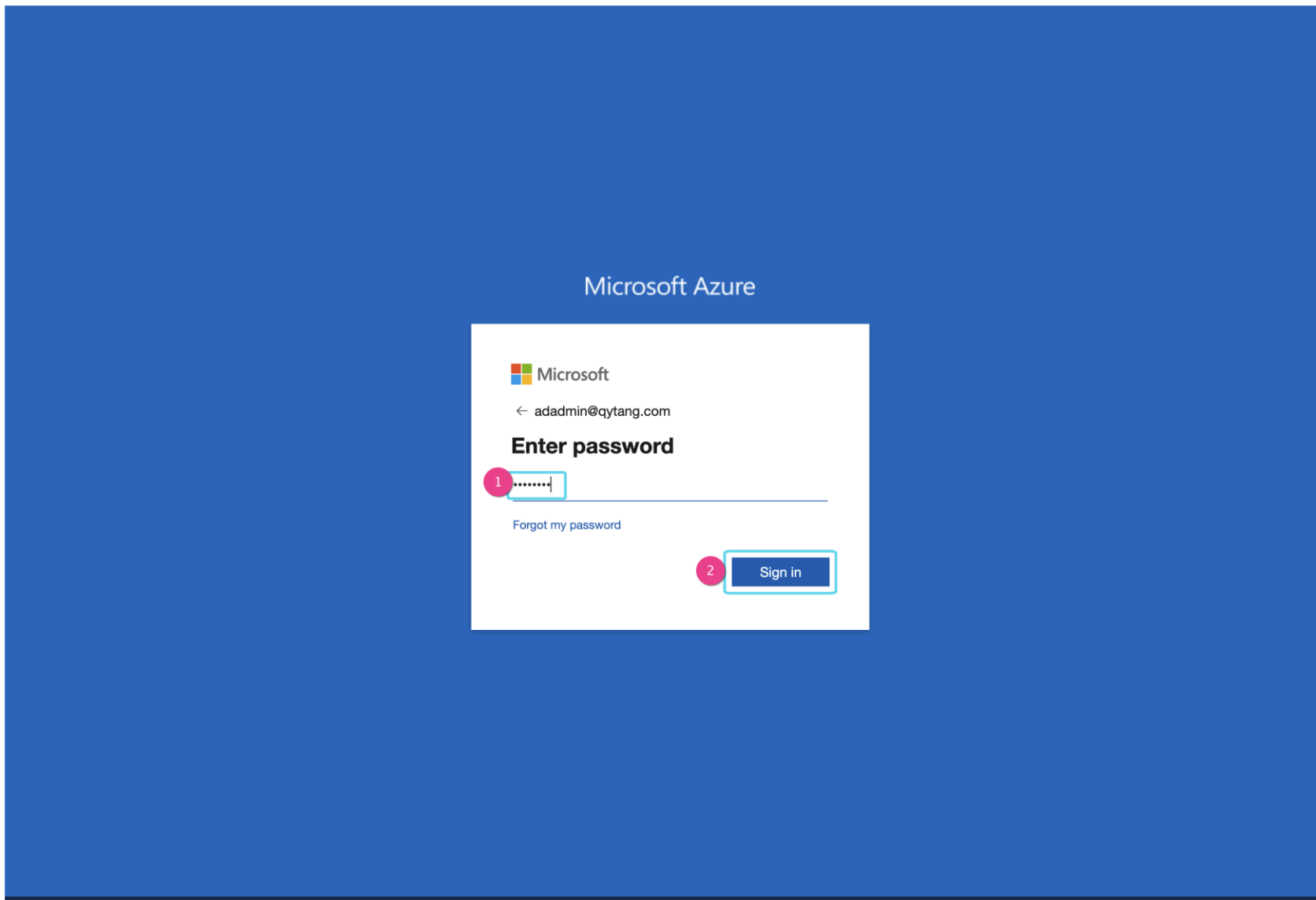


初始化管理员



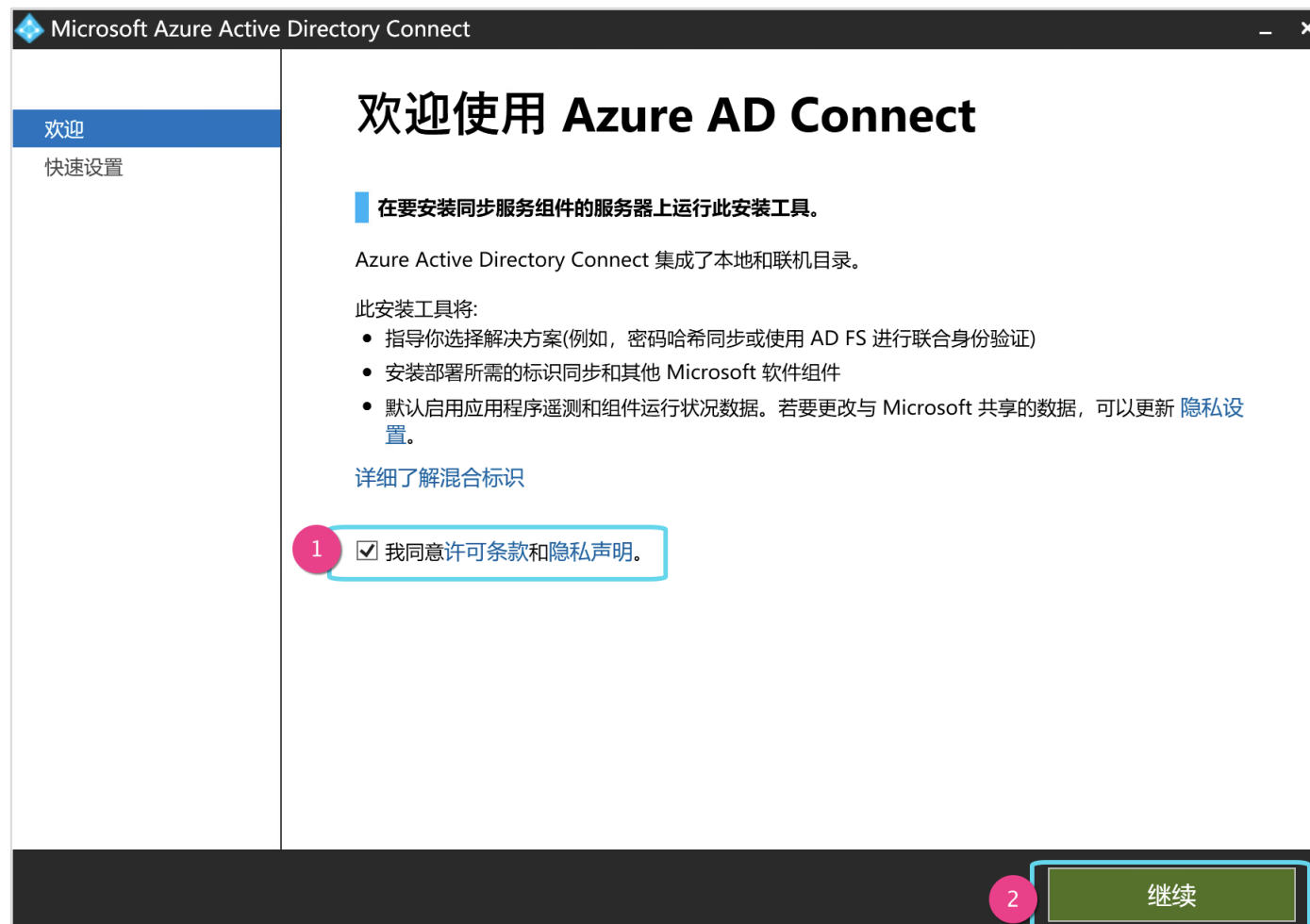


初始化管理员





安装并连接





安装并连接

Microsoft Azure Active Directory Connect

欢迎

快速设置

快速设置

如果您有单个 Windows Server Active Directory 林，将执行以下操作:

- 配置 QYTANG 的当前 AD 林的标识同步
- 配置从本地 AD 到 Azure AD 的密码哈希同步
- 启动初始同步
- 同步所有属性
- 启用自动升级

[了解有关快速设置的更多信息](#)

选择“自定义”，以选择高级部署选项或从现有服务器中导入设置。

自定义 使用快速设置



安装并连接

Microsoft Azure Active Directory Connect

欢迎

快速设置

连接到 Azure AD

连接到 AD DS

配置

连接到 Azure AD

输入 Azure AD 全局管理员或混合标识管理员凭据。 ?

1 用户名
adadmin@qytang.com

2 密码
.....

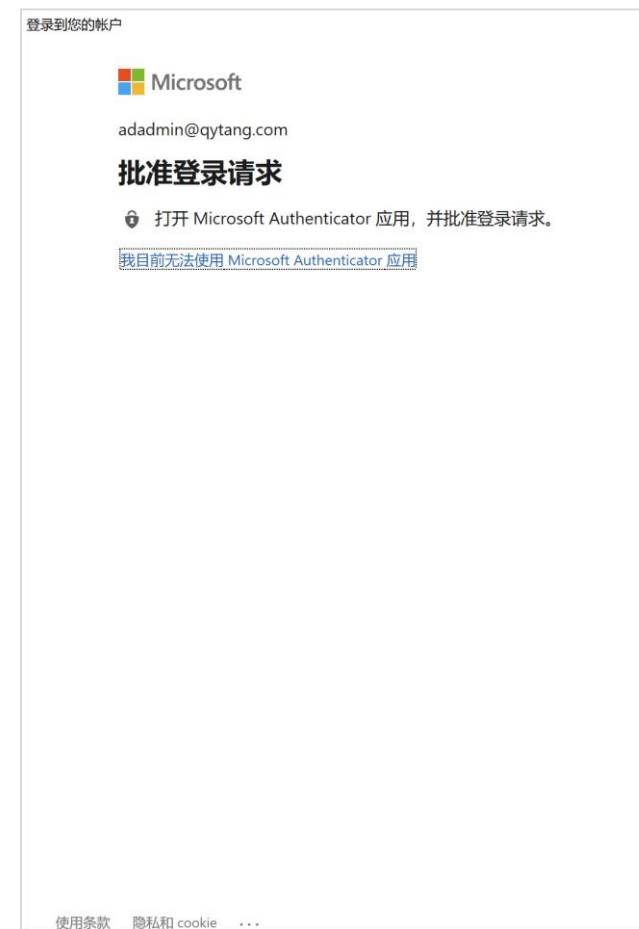
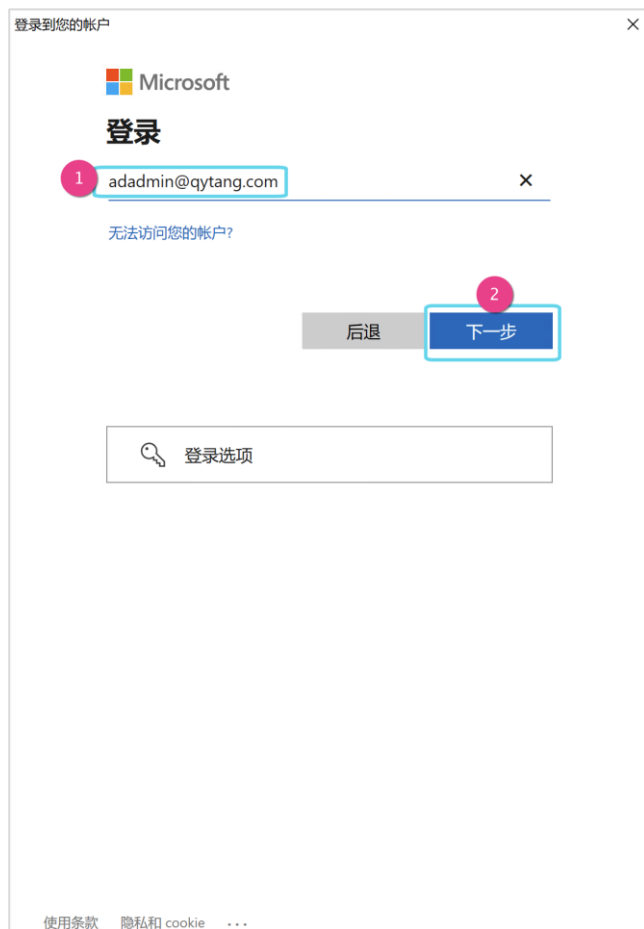
正在连接到 Microsoft Online 以验证凭据。

3 下一步

上一步



安装并连接





安装并连接

Microsoft Azure Active Directory Connect

欢迎
快速设置
连接到 Azure AD
连接到 AD DS
配置

连接到 AD DS

输入 Active Directory 域服务企业管理员凭据: ?

1 用户名
QYTANG\administrator

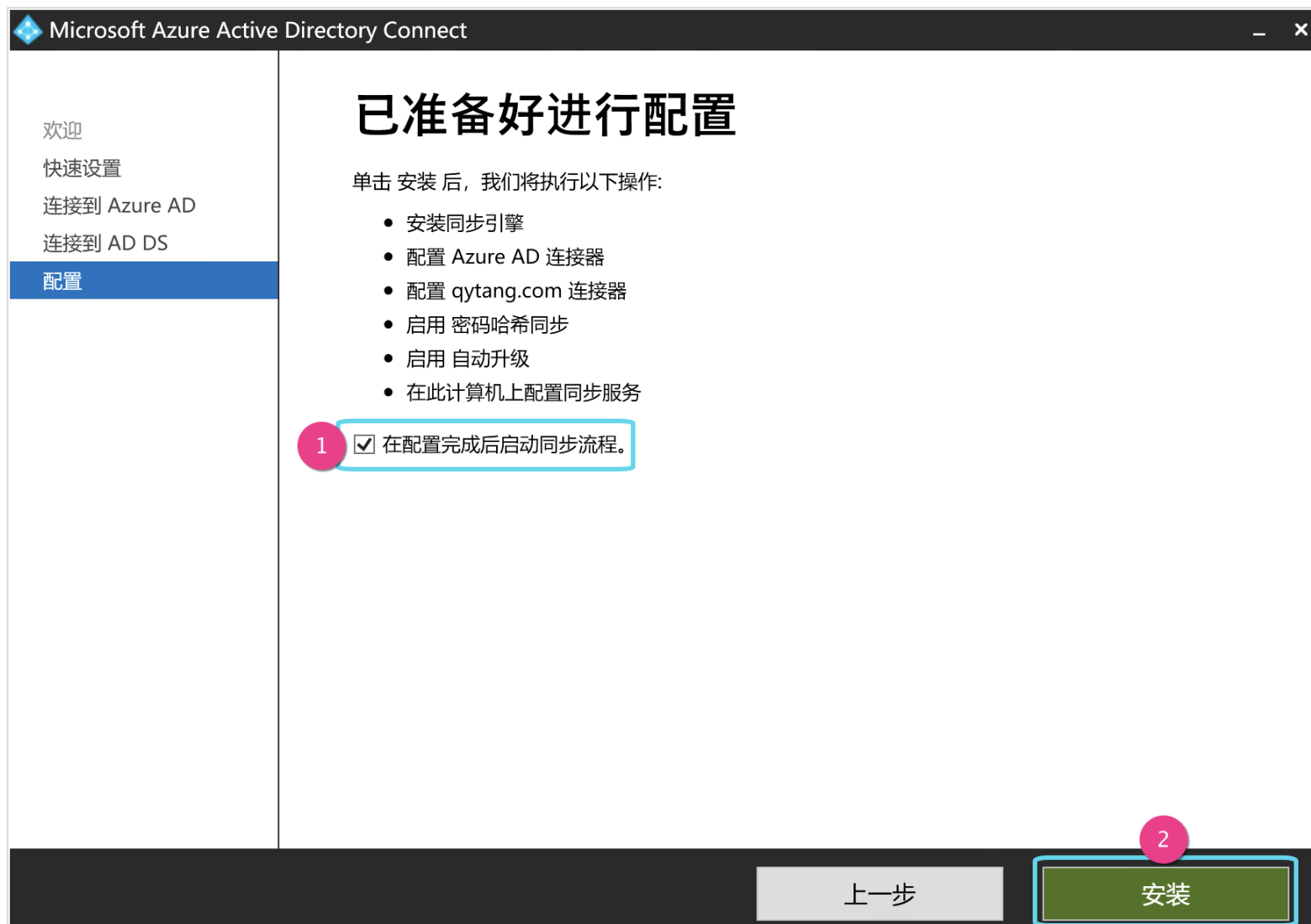
2 密码
●●●●●●

3 下一步

上一步

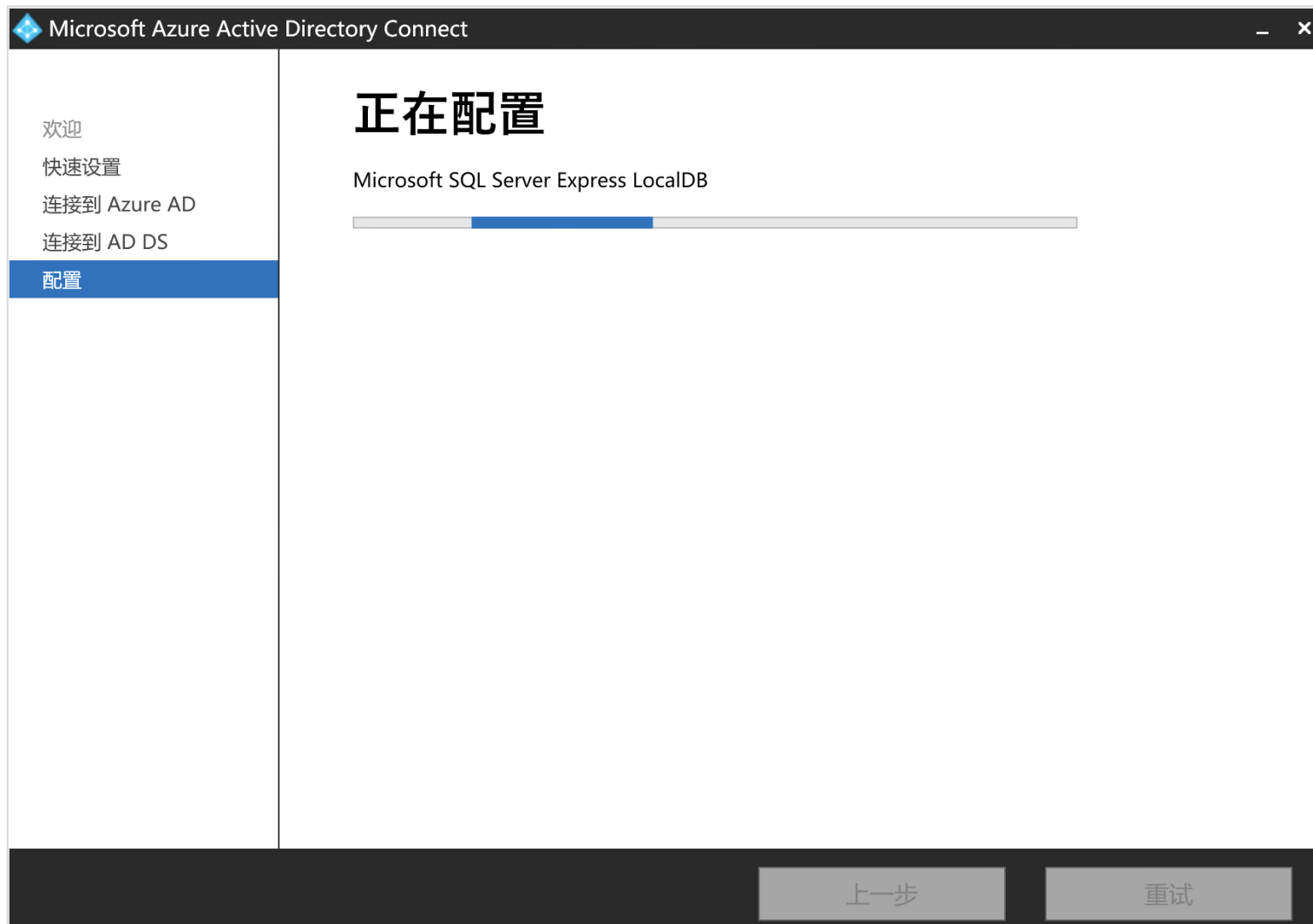


安装并连接





安装并连接





安装并连接

Microsoft Azure Active Directory Connect

欢迎

快速设置

连接到 Azure AD

连接到 AD DS

配置

配置完成

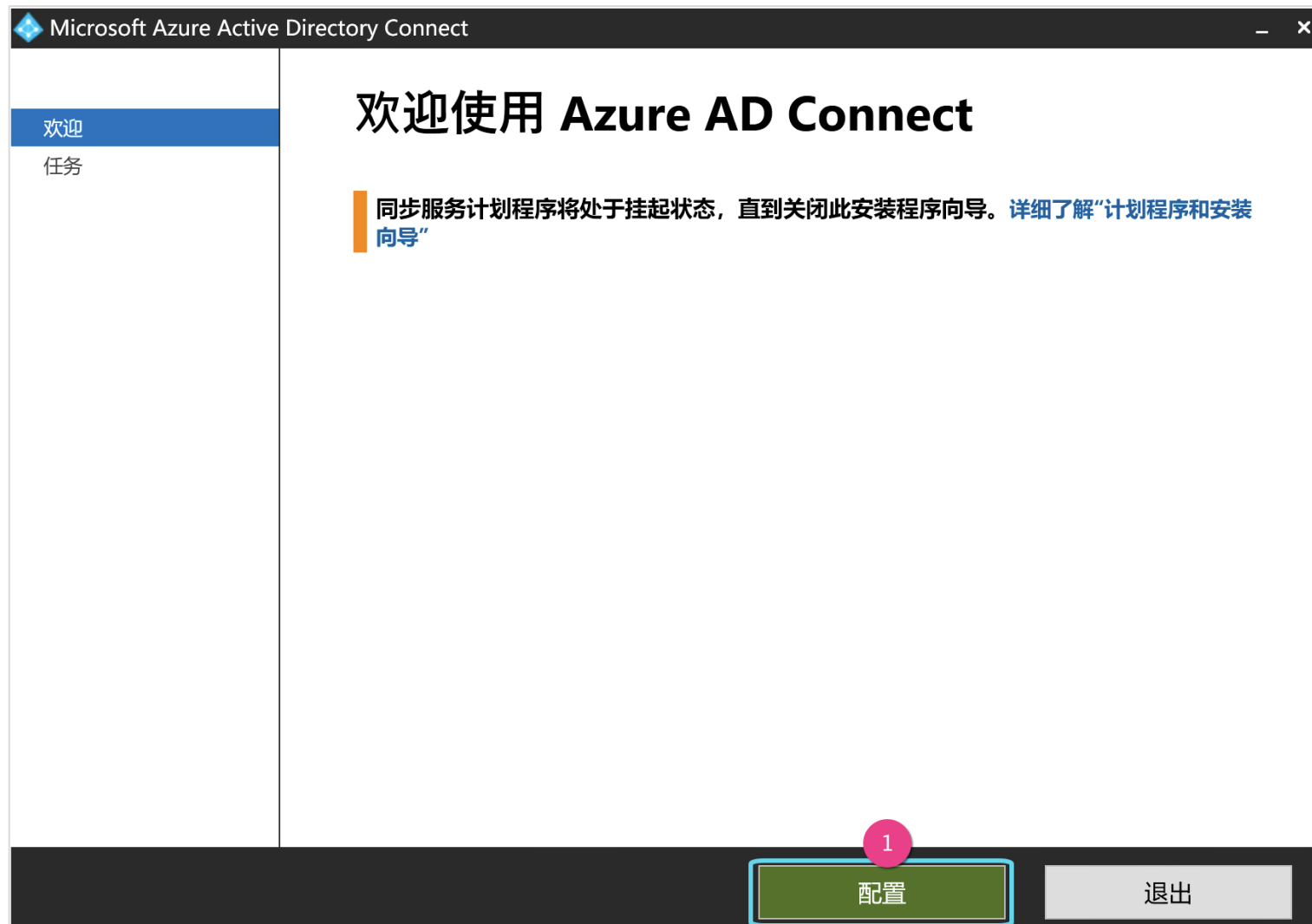
Azure AD Connect 配置成功。同步过程已启动。

- 配置已完成。你可以立即登录到 Azure 或 Office 365 门户，以验证是否已从本地目录创建用户帐户。随后，测试登录到 Azure 门户。[详细了解后续步骤和如何管理 Azure AD Connect](#)
- 没有为林(qytang.com)启用 Active Directory 回收站，强烈建议启用回收站。[详细了解如何启用 Active Directory 回收站](#)
- Azure Active Directory 配置为使用 AD 属性 `mS-DS-ConsistencyGuid` 作为源定位属性。[详细了解如何配置源定位点属性](#)

上一步 退出



配置同步





配置同步

Microsoft Azure Active Directory Connect

欢迎

任务

其他任务

方案所需的任务已完成。请从以下列表中进行选择以执行其他任务。

- 隐私设置
- 查看或导出当前配置
- 1 自定义同步选项
- 配置设备选项 ?
- 刷新目录架构
- 配置暂存模式
- 更改用户登录
- 管理联合身份验证服务 ?
- 疑难解答

2

上一步

下一步



配置同步

Microsoft Azure Active Directory Connect

连接到 Azure AD

为 collinsctkqytang.onmicrosoft.com - AAD 输入 Azure AD 全局管理员或混合标识管理员凭据。 ?

1 用户名
adadmin@qytang.com

2 密码
●●●●●●●●●●

3 下一步



配置同步

Microsoft Azure Active Directory Connect

欢迎
任务
连接到 Azure AD
同步
连接目录
域/OU 筛选
可选功能
配置

连接目录

输入本地目录或林的连接信息。 ?

目录类型
Active Directory

林 ?
qytang.com 添加目录

配置的目录
qytang.com (Active Directory) ✓

1
上一步 下一步



配置同步

Microsoft Azure Active Directory Connect

欢迎
任务
连接到 Azure AD
同步
连接目录
域/OU 筛选
可选功能
配置

域和 OU 筛选

如果更改给定目录的 OU 筛选配置，则下一个同步周期将自动在目录上执行完全导入。

目录: ?

同步所有域和 OU
 同步选定的域和 OU

1

2

- qytang.com
 - ADFS
 - Builtin
 - Computers
 - Domain Controllers
 - ForeignSecurityPrincipals
 - Infrastructure
 - LostAndFound
 - Managed Service Accounts
 - Program Data
 - System
 - Users



配置同步

Microsoft Azure Active Directory Connect

欢迎
任务
连接到 Azure AD
同步
 连接目录
 域/OU 筛选
 可选功能
配置

可选功能

如果组织需要，请选择增强功能。

- Exchange 混合部署 ?
- Exchange 邮件公用文件夹 ?
- Azure AD 应用和属性筛选 ?
- 1** 密码哈希同步 ?
- 密码写回 ?
- 组写回 ⚠
- 设备写回 ?
- 目录扩展属性同步 ?

有关可选功能的[了解更多](#)。

2 下一步

上一步



配置同步

Microsoft Azure Active Directory Connect

欢迎
任务
连接到 Azure AD
同步
 连接目录
 域/OU 筛选
 可选功能
配置

已准备好进行配置

正在确认已安装的组件

上一步 配置



配置同步

Microsoft Azure Active Directory Connect

欢迎
任务
连接到 Azure AD
同步
连接目录
域/OU 筛选
可选功能
配置

已准备好进行配置

单击 配置 后, 我们将执行以下操作:

- 更新 qytang.com 连接器
- 在此计算机上配置同步服务

在配置完成后启动同步流程。

上一步 配置



配置同步

Microsoft Azure Active Directory Connect

正在配置

更新 (qytang.com)

配置

上一步 重试



配置同步

Microsoft Azure Active Directory Connect

欢迎
任务
连接到 Azure AD
同步
 连接目录
 域/OU 筛选
 可选功能
配置

配置完成

Azure AD Connect 配置成功。同步过程已启动。

配置已完成。你可以立即登录到 Azure 或 Office 365 门户，以验证是否已从本地目录创建用户帐户。随后，测试登录到 Azure 门户。 [详细了解后续步骤和如何管理 Azure AD Connect](#)

上一步 退出



查看同步的用户

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

Home > Default Directory > 1

Users | All users ...

Default Directory - Azure Active Directory

+ New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user Columns Got feedback?

Search users Add filters

4 users found

Name	User principal na...↑↓	User type	Directory synced	Account enabled	Identity issuer	Company name	Creation type
<input type="checkbox"/> AD adadmin	adadmin@qytang.com	Member	No	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/> AD adfsuser	adfsuser@qytang.com	Member	Yes	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/> OD On-Premises ...	Sync_QYTWIN2019_6...	Member	Yes	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/> 秦柯 秦柯	collinsctk_qytang.co...	Member	No	Yes	MicrosoftAccount		

Activity

- Sign-in logs
- Audit logs
- Bulk operation results

Troubleshooting + Support

- New support request



查看同步的组

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

Home > Default Directory > 1

Groups | All groups

Default Directory - Azure Active Directory

New group Download groups Delete Refresh Columns Got feedback?

Search Add filter

Search mode Contains

7 groups found

<input type="checkbox"/>	Name ↑	Object Id	Group type	Membership type	Email
<input checked="" type="checkbox"/>	AD adfs_group	a08446ef-f813-47b0-b072-ba6a19111d09	Security	Assigned	
<input type="checkbox"/>	ADSyncAdmins	286ffdd3-1c72-4326-a960-e6792f24d6bf	Security	Assigned	
<input type="checkbox"/>	ADSyncBrowse	5cfd8a65-0d59-49bd-877d-0f3980ea03cb	Security	Assigned	
<input type="checkbox"/>	ADSyncOperators	b18e2a7e-83b7-4b22-9261-18514e4e23f1	Security	Assigned	
<input type="checkbox"/>	ADSyncPasswordSet	a14cbe41-2030-4912-b22e-3395c5a64d92	Security	Assigned	
<input type="checkbox"/>	QY qytang-admin-group	cea63242-3493-497c-83dc-f3f746b50cd5	Security	Assigned	
<input type="checkbox"/>	US usergroup1	fbd3a991-9257-4a8c-bc27-7ed68cb83642	Security	Assigned	

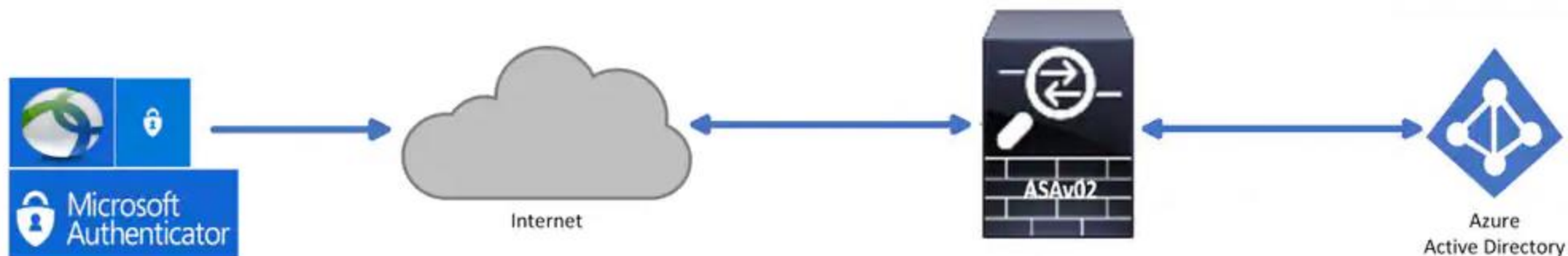
SAML





Cisco AnyConnect SAML

Network Diagram



<https://www.cisco.com/c/en/us/support/docs/security/anyconnect-secure-mobility-client/215935-configure-asa-anyconnect-vpn-with-micros.html>

参考文档



Azure创建企业应用

1

2

Search resources, services, and docs (G+)

collinsctk@qytang.com
DEFAULT DIRECTORY

ry | Overview ...

+ Add Manage tenants What's new Preview features Got feedback?

Overview Monitoring Tutorials

Search your tenant

Basic information

Name	Default Directory	Users	3
Tenant ID	9a2af509-1e76-4091-9cbc-5286f5db8e7a	Groups	2
Primary domain	qytang.com	Applications	28
License	Azure AD Free	Devices	8

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation
Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.
[Learn more](#)

My feed

柯素
977a0491-548e-47f6-8f63-f83b5ebfe487
Global administrator
[View role information](#)

Secure Score for Identity
28.57%
Secure score updates can take up to 48 hours.

Azure AD Connect
Not enabled
Sync has never run



Azure创建企业应用

Microsoft Azure

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

Home >

Default Directory | Overview

Azure Active Directory

External Identities

Roles and administrators

Administrative units

Enterprise applications

Devices

App registrations

Identity Governance

Application proxy

Custom security attributes (Preview)

Licenses

Azure AD Connect

Custom domain names

Mobility (MDM and MAM)

Password reset

User settings

Properties

Security

Monitoring

Sign-in logs

Audit logs

Provisioning logs

+ Add

Manage tenants

What's new

Preview features

Got feedback?

Overview

Monitoring

Tutorials

Search your tenant

Basic information

Name	Default Directory	Users	3
Tenant ID	9a2af509-1e76-4091-9cbc-5286f5db8e7a	Groups	2
Primary domain	qytang.com	Applications	28
License	Azure AD Free	Devices	8

Alerts

Upcoming TLS 1.0, 1.1 and 3DES deprecation

Please enable support for TLS 1.2 on clients(applications/platform) to avoid any service impact.

[Learn more](#)

My feed

柯素

977a0491-548e-47f6-8f63-f83b5ebfe487

Global administrator

[View role information](#)

Secure Score for Identity

28.57%

Secure score updates can take up to 48 hours.

Azure AD Connect

Not enabled

Sync has never run



Azure创建企业应用

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > Enterprise applications

Enterprise applications | All applications

Default Directory - Azure Active Directory

+ New application 1 fresh Download (Preview) Preview info Columns Preview features Got feedback?

View, filter, and search applications in your organization that are set up to use your Azure AD tenant as their Identity Provider.

Search by application name or object ID Application type == Enterprise Applications Applications status == Any Application visibility == Any Add filters

0 applications found

Name	Object ID	Application ID	Homepage URL	Created on
No results				

Overview

- Overview
- Diagnose and solve problems

Manage

- All applications
- Application proxy
- User settings
- Collections

Security

- Conditional Access
- Consent and permissions

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews
- Admin consent requests
- Bulk operation results

Troubleshooting + Support



Azure创建企业应用

Microsoft Azure

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

collinsck@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications >

Browse Azure AD Gallery

+ Create your own application | Request new gallery app | Got feedback?


The Azure AD App Gallery is a catalog of thousands of apps that make it easy to deploy and configure single sign-on (SSO) and automated user provisioning. When deploying an app from the App Gallery, create your own application here.


anyconnect 1


Single Sign-on : All | User Account Management : All | Categories : All


Federated SSO | Provisioning


Showing 9 of 9 results 2


 **Cisco AnyConnect**
Cisco Systems, Inc.


 **mConnect**
Skooler AS


 **Connector**
Design Connected

 **SafeCo**
Impulse

 **Pobuca Connect**
Pobuca

 **i2B Connect**
i2B Limited

 **Taskize Connect**
Taskize

 **Traced**
Traced Lt

Cisco AnyConnect

Got feedback?

Logo ¹

Name * ¹
Cisco AnyConnect

Publisher ¹
Cisco Systems, Inc.

Provisioning ¹
Automatic provisioning is not supported

Single Sign-On Mode ¹
SAML-based Sign-on
Linked Sign-on

URL ¹
https://www.ciscoanyconnect.com/

[Read our step-by-step Cisco AnyConnect integration tutorial](#)

Empower your employees to work from anywhere, on company laptops or personal mobile devices, at any time. AnyConnect simplifies secure endpoint access and provides the security necessary to help keep your organization safe and protected.

Create 3



配置SAML

The screenshot displays the Microsoft Azure portal interface for configuring Cisco AnyConnect. The top navigation bar includes the Microsoft Azure logo, a search bar, and the user's email address (collinsctk@qytang.com). The breadcrumb trail indicates the path: Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect | Overview.

The left-hand navigation pane lists various management options: Overview (selected), Deployment Plan, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on, Provisioning, Self-service, Custom security attributes (preview), Security, Conditional Access, Permissions, Token encryption, Activity, Sign-in logs, Usage & insights, and Audit logs.

The main content area is titled "Cisco AnyConnect | Overview" and features a "Properties" section with the following details:

- Name: Cisco AnyConnect
- Application ID: f8cb5fef-0e7c-4b26-8aff-f4...
- Object ID: 453298b4-c96e-4d02-9be6-...

Below the properties is the "Getting Started" section, which contains five numbered steps:

- 1. Assign users and groups**: Provide specific users and groups access to the applications. [Assign users and groups](#)
- 2. Set up single sign on**: Enable users to sign into their application using their Azure AD credentials. [Get started](#)
- 3. Provision User Accounts**: You'll need to create user accounts in the application. [Learn more](#)
- 4. Conditional Access**: Secure access to this application with a customizable access policy. [Create a policy](#)
- 5. Self service**: Enable users to request access to the application using their Azure AD credentials. [Get started](#)

The "What's New" section is partially visible at the bottom of the page.



配置SAML

Microsoft Azure

Search resources, services, and docs (G+)

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect

Cisco AnyConnect | Single sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Self-service
 - Custom security attributes (preview)
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling a user in your organization to sign in to every application they use with only one account. Once the user logs into an application, that credential is used for all the other applications they need access to. [Learn more](#).

Select a single sign-on method [Help me decide](#)

- Disabled**
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.
- SAML**
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.
- Linked**
Link to an application in My Apps and/or Office 365 application launcher.



配置SAML

Microsoft Azure

Search resources, services, and docs (G+)

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect >

Cisco AnyConnect | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Cisco AnyConnect.

- #### Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- #### Attributes & Claims

⚠ Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- #### SAML Signing Certificate

⚠ Fill out required fields in Step 1

Status	Active
--------	--------



配置SAML

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

Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect >

Cisco AnyConnect | SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes (preview)
Security
Conditional Access
Permissions
Token encryption
Activity
Sign-in logs
Usage & insights
Audit logs

Upload metadata file | Change single sign-on mode | Test this application | Got feedback

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experience. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID more.

Read the [configuration guide](#) for help integrating Cisco AnyConnect.

- Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- Attributes & Claims

Fill out required fields in Step 1

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- SAML Signing Certificate

Fill out required fields in Step 1

Status	Active
--------	--------

Basic SAML Configuration

Save | Got feedback?

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) * ⓘ
The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant.

2

1 Add identifier

Patterns: https://*.YourCiscoServer.com/saml/sp/metadata/TGTGroup

https://asa.qytang.com/saml/sp/metadata/qytang-anyconnect

Reply URL (Assertion Consumer Service URL) * ⓘ
The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

4

3 Add reply URL

Patterns: https://YOUR_CISCO_ANYCONNECT_FQDN/+CSCOE+/SAML/SP/ACS

https://asa.qytang.com/+CSCOE+/saml/sp/acs?tgname=qytang-anyconnect

Sign on URL (Optional) ⓘ
Sign on URL is used if you would like to perform service provider-initiated single sign-on. This value is the sign-in page URL for your application. This field is unnecessary if you want to perform identity provider-initiated single sign-on.

Relay State (Optional) ⓘ
The Relay State instructs the application where to redirect users after authentication is completed, and the value is typically a URL or URL path that takes users to a specific location within the application.



URL介绍

Entity ID: This field is a unique identifier for an SP or an IdP. A single device might have several services and can use different Entity IDs to differentiate them. For example, **ASA has different Entity IDs for different tunnel-groups that need to be authenticated**[每一个tunnel-group一个Entity ID]. An IdP authenticating each tunnel-group has a separate Entity ID entries for each tunnel-group in order to accurately identify those services.

Identifier (Entity ID) : `https://<VPN URL>/saml/sp/metadata/<TUNNEL-GROUP NAME>`

The Assertion Consumer Service URL found in the SP metadata is used by **the IdP to redirect the user back to the SP and provide information about the user's authentication attempt**[IDP重定向用户返回SP,并且提供用户认证的信息]. If this is configured incorrectly, the SP does not receive the assertion (the response) or is unable to successfully process it.

Reply URL (Assertion Consumer Service URL) : `https://<VPN URL>/+CSCOE+/saml/sp/acs?tgname=<TUNNEL-GROUP NAME>`



配置SAML

Microsoft Azure

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

Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect >

Cisco AnyConnect | SAML-based Sign-on

Enterprise Application

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. [Learn more.](#)

Read the [configuration guide](#) for help integrating Cisco AnyConnect.

- #### Basic SAML Configuration

Identifier (Entity ID)	https://asa.qytang.com/saml/sp/metadata/qytang-anyconnect
Reply URL (Assertion Consumer Service URL)	https://asa.qytang.com/+CSCOE+/saml/sp/acs?tgname=qvtang-anyconnect
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional
- #### Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname
- #### SAML Signing Certificate

Status	Active
Thumbprint	4C45FFCECE6A7BE8B69A71152D78B16D718C217E

下载Azure证书

Microsoft Azure

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

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect >

Cisco AnyConnect | SAML-based Sign-on

Enterprise Application

Overview
Deployment Plan

Manage

- Properties
- Owners
- Roles and administrators
- Users and groups
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

3 SAML Signing Certificate [Edit](#)

Status	Active
Thumbprint	4C45FFCECE6A7BE8B69A71152D78B16D718C217E
Expiration	4/11/2025, 2:28:10 PM
Notification Email	collinsctk@qytang.com
App Federation Metadata Url	https://login.microsoftonline.com/9a2af509-1e76-...
Certificate (Base64)	Download 1
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Cisco AnyConnect

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/9a2af509-1e76-...
Azure AD Identifier	https://sts.windows.net/9a2af509-1e76-4091-9cbc...
Logout URL	https://login.microsoftonline.com/9a2af509-1e76-...

[View step-by-step instructions](#)

5 Test single sign-on with Cisco AnyConnect

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#)

Cisco AnyConnec....cer 2

Show all

后续要在ASA上加载此证书

```
crypto ca trustpoint Azure-SAML
revocation-check none
no id-usage
enrollment terminal
no ca-check

crypto ca authenticate Azure-SAML
-----BEGIN CERTIFICATE-----

~~~下载的Cisco AnyConnect的证书~~~

-----END CERTIFICATE-----

quit
```



配置SAML

Microsoft Azure

Home > Default Directory > Enterprise applications > Browse Azure AD Gallery > Cisco AnyConnect >

Cisco AnyConnect | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on
 - Provisioning
 - Self-service
 - Custom security attributes (preview)
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs

Upload metadata file | Change single sign-on mode | Test this application | Got feedback?

3 SAML Signing Certificate Edit

Status	Active
Thumbprint	4C45FFCECE6A7BE8B69A71152D78B16D718C217E
Expiration	4/11/2025, 2:28:10 PM
Notification Email	collinsctk@qytang.com
App Federation Metadata Url	https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Cisco AnyConnect

You'll need to configure the application to link with Azure AD.

1

Login URL: <https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/saml2>

Azure AD Identifier: <https://sts.windows.net/9a2af509-1e76-4091-9cbc-5286f5db8e7a/>

Logout URL: <https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/>

[View step-by-step instructions](#)

5 Test single sign-on with Cisco AnyConnect

Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in.

[Test](#) 创建用户后Test验证

9a2af509-1e76-4091-9cbc-5286f5db8e7a
是租户的唯一ID

login/logout是一样的

Copy it, and configure it in asa later

<https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/saml2>

<https://sts.windows.net/9a2af509-1e76-4091-9cbc-5286f5db8e7a/>

<https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/>



URL介绍

Azure AD Identifier: **Service URLs**: These define the URL to a SAML service provided by the SP or IdP.

Login URL : The **Single Sign-On Service URL** found in the IdP metadata is used by the SP to **redirect the user to the IdP for authentication**[SP重定向用户到IDP认证]. If this value is incorrectly configured, the IdP does not receive or is unable to successfully process the Authentication request sent by the SP.

Logout URL : The **Single Logout Service URL** can be found on both the SP and the IdP. It is used to facilitate logging out of all SSO services from the SP and is optional on the ASA. When the SLO service URL from the IdP metadata is configured on the SP, **when the user logs out of the service on the SP, the SP sends the request to the IdP**[当用户从SP登出, SP发送通知到IDP]. Once the IdP has successfully logged the user out of the services, it redirects the user back to the SP using the SLO service URL found within the SP's metadata.



查看用户

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

Home > Default Directory > 1

Users | All users ...

Default Directory - Azure Active Directory

All users 2 Deleted users Password reset User settings Diagnose and solve problems Activity Sign-in logs Audit logs Bulk operation results Troubleshooting + Support New support request

+ New user + New guest user Bulk operations Refresh Reset password Per-user MFA Delete user Columns Got feedback?

Search users Add filters

4 users found

	Name	User principal na...↑↓	User type	Directory synced	Account enabled	Identity issuer	Company name	Creation type
<input type="checkbox"/>	AD adadmin	adadmin@qytang.com	Member	No	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/>	AD adfsuser	adfsuser@qytang.com	Member	Yes	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/>	OD On-Premises ...	Sync_QYTWIN2019_f...	Member	Yes	Yes	collinsctkqytang.onmicr		
<input type="checkbox"/>	秦柯	collinsctk_qytang.co...	Member	No	Yes	MicrosoftAccount		

用户无需创建, 已经被AD Connect自动同步



为企业应用指派用户

The screenshot shows the Microsoft Azure portal interface for managing Cisco AnyConnect users and groups. The breadcrumb navigation at the top is highlighted with a red box and a red circle containing the number 1. The left-hand navigation pane has the 'Users and groups' option highlighted with a red box and a red circle containing the number 2. The main content area features a toolbar with the 'Add user/group' button highlighted by a red box and a red circle containing the number 3. Below the toolbar, there is a search bar and a table with columns for 'Display Name', 'Object Type', and 'Role assigned'. The table currently displays 'No application assignments found'.

Microsoft Azure

Search resources, services, and docs (G+)

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > Cisco AnyConnect

Cisco AnyConnect | Users and groups

Enterprise Application

Overview
Deployment Plan

Manage

Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Self-service
Custom security attributes (preview)

Security

Conditional Access
Permissions
Token encryption

Activity

Sign-in logs
Usage & insights
Audit logs

+ Add user/group edit Remove Update Credentials Columns Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
No application assignments found		



为企业应用指派用户

Microsoft Azure

Search resources, services, and docs (G+)

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > Cisco AnyConnect >

Add Assignment

Default Directory

⚠ Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

None Selected **1**

Select a role

Default Access

Assign

由于授权原因只能指派单个用户,不能指派组



为企业应用指派用户

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

Home > Default Directory > Enterprise applications > Cisco AnyConnect >

Add Assignment

Default Directory

Warning: Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

None Selected

Select a role

Default Access

Assign

Users

Search

- 秦柯 collinsctk@qytang.com
- adadmin adadmin@qytang.com
- AD adfsuser@qytang.com** Selected
- On-Premises Directory Synchronization Service Account Sync_QYTWIN2019_f52740b86aeb@collinsctkqytang.onmicrosoft.com

Selected items

- AD adfsuser@qytang.com** Remove

Select



为企业应用指派用户

Microsoft Azure

Search resources, services, and docs (G+)

Home > Default Directory > Enterprise applications > Cisco AnyConnect >

Add Assignment

Default Directory

Groups are not available for assignment due to your Active Directory plan level. You can assign individual users to the application.

Users

1 user selected.

Select a role

Default Access

Assign 4



为企业应用指派用户

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

Home > Default Directory > Enterprise applications > Cisco AnyConnect

Cisco AnyConnect | Users and groups ...
Enterprise Application

Application assignment succeeded
1 user & 0 groups have been assigned access

« + Add user/group Edit Remove Update Credentials Columns Got feedback?

The application will appear for assigned users within My Apps. Set 'visible to users?' to no in properties to prevent this. →

First 200 shown, to search all users & groups, enter a display name.

Display Name	Object Type	Role assigned
<input type="checkbox"/> AD adfsuser	User	Default Access

Manage

- Overview
- Deployment Plan
- Properties
- Owners
- Roles and administrators
- Users and groups**
- Single sign-on
- Provisioning
- Self-service
- Custom security attributes (preview)

Security

- Conditional Access
- Permissions
- Token encryption

Activity

- Sign-in logs
- Usage & insights
- Audit logs
- Provisioning logs
- Access reviews



测试用户

The screenshot shows the Microsoft Azure portal interface for configuring Cisco AnyConnect SAML-based Sign-on. The breadcrumb navigation at the top is: Home > Default Directory > Enterprise applications > Cisco AnyConnect > 1. The main title is "Cisco AnyConnect | SAML-based Sign-on".

The left-hand navigation pane includes sections for Overview, Deployment Plan, Manage, Properties, Owners, Roles and administrators, Users and groups, Single sign-on (highlighted with a red box and number 2), Provisioning, Self-service, Custom security attributes (preview), Security, Conditional Access, Permissions, Token encryption, and Activity. Under Activity, "Sign-in logs" is highlighted with a red box and number 2.

The main content area has a top bar with links: Upload metadata file, Change single sign-on mode, Test this application, and Got feedback?. Below this are three main sections:

- 3 SAML Signing Certificate**: A table showing certificate details. The "Status" is Active. The "Thumbprint" is 4C45FFCECE6A7BE8B69A71152D78B16D718C217E. The "Expiration" is 4/11/2025, 2:28:10 PM. The "Notification Email" is collinsctk@qytang.com. The "App Federation Metadata Url" is https://login.microsoftonline.com/9a2af509-1e76-... (truncated). There are links for "Certificate (Base64)", "Certificate (Raw)", and "Federation Metadata XML", all labeled "Download".
- 4 Set up Cisco AnyConnect**: A section titled "Set up Cisco AnyConnect" with the instruction: "You'll need to configure the application to link with Azure AD." It lists "Login URL", "Azure AD Identifier", and "Logout URL", each with a truncated URL and a "Copy" icon. A link for "View step-by-step instructions" is also present.
- 5 Test single sign-on with Cisco AnyConnect**: A section titled "Test single sign-on with Cisco AnyConnect" with the instruction: "Test to see if single sign-on is working. Users will need to be added to Users and groups before they can sign in." A blue "Test" button is highlighted with a red box and number 3.



测试用户

Microsoft Azure

Search resources, services, and docs (G+)

collinsctk@qytang.com
DEFAULT DIRECTORY

Home > Default Directory > Enterprise applications > Cisco AnyConnect >

Cisco AnyConnect | SAML-based Sign-on

Enterprise Application

- Overview
- Deployment Plan
- Manage
 - Properties
 - Owners
 - Roles and administrators
 - Users and groups
 - Single sign-on**
 - Provisioning
 - Self-service
 - Custom security attributes (preview)
- Security
 - Conditional Access
 - Permissions
 - Token encryption
- Activity
 - Sign-in logs
 - Usage & insights
 - Audit logs

Upload metadata file | Change single sign-on mode | Test this application | Got feedback

3 SAML Signing Certificate

Status	Active
Thumbprint	4C45FFCECE6A7BE8B69A71152D78B16D718C217E
Expiration	4/11/2025, 2:28:10 PM
Notification Email	collinsctk@qytang.com
App Federation Metadata Url	https://login.microsoftonline.com/9a2af509-1e76-4091-9cb0-000000000000/9a2af509-1e76-4091-9cb0-000000000000
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

4 Set up Cisco AnyConnect

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/9a2af509-1e76-4091-9cb0-000000000000/9a2af509-1e76-4091-9cb0-000000000000
Azure AD Identifier	https://sts.windows.net/9a2af509-1e76-4091-9cb0-000000000000/
Logout URL	https://login.microsoftonline.com/9a2af509-1e76-4091-9cb0-000000000000/9a2af509-1e76-4091-9cb0-000000000000

[View step-by-step instructions](#)

5 Test single sign-on with Cisco AnyConnect

Test to see if single sign-on is working. Users will need to be added to Users and groups before the test.

[Test](#)

Test single sign-on with Cisco AnyConnect

需要安装浏览器扩展

Got feedback?

Testing sign in

Test the single sign-on configuration for Cisco AnyConnect by signing in here. Ensure that you have configured both the Azure Active Directory configuration and Cisco AnyConnect itself.

Select a way to test sign in

Sign in as current user

Sign in as someone else (requires browser extension) 1

[Test sign in](#) 2

Resolving errors

If you encounter an error in the sign-in page, please paste it below. If you still see the same issue, please wait for couple of minutes and retry.

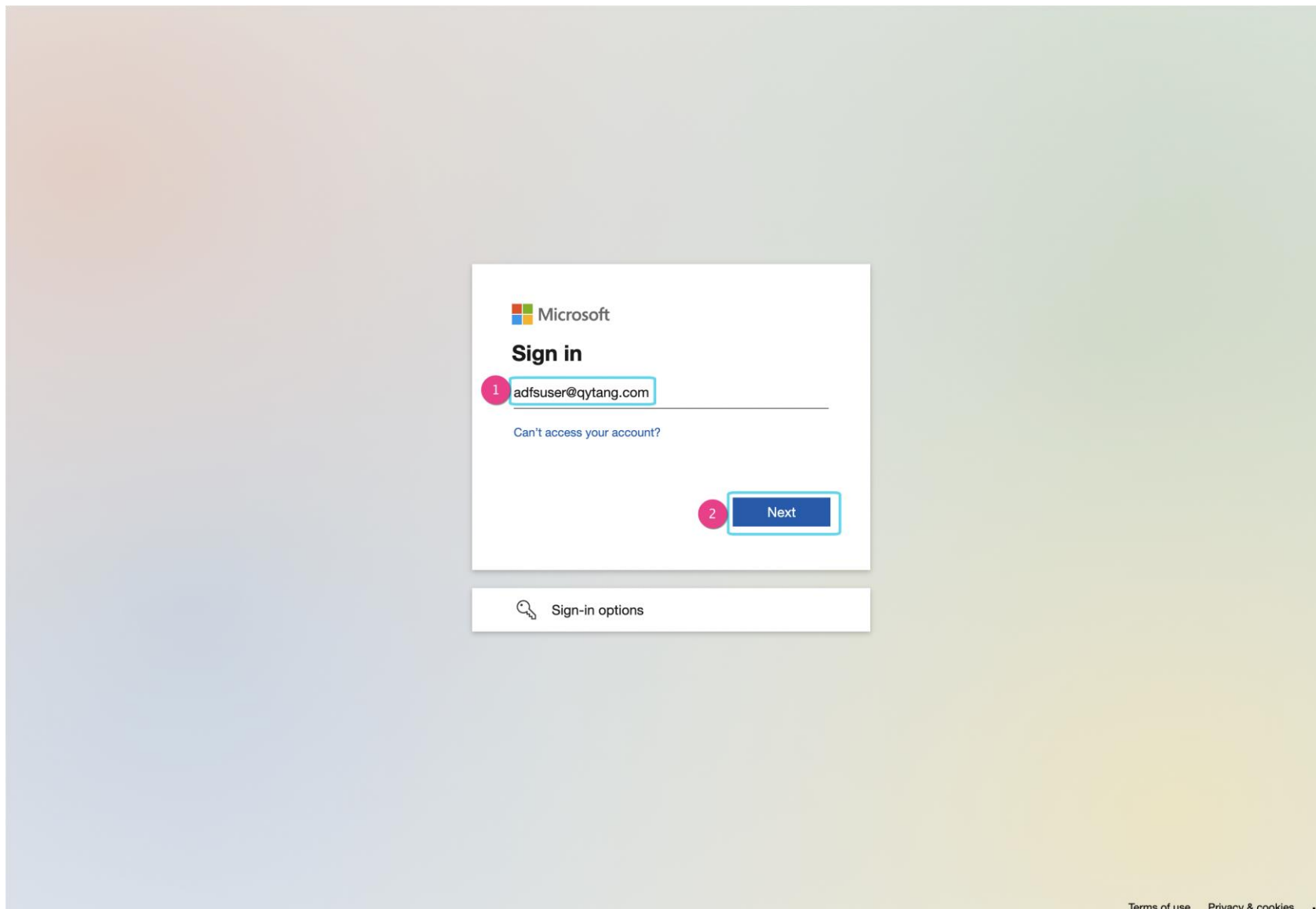
What does the error look like? [↗](#)

```
Request Id: 4f8ec053-fb71-47de-a010-2786a32f1900
Correlation Id: 5aa879f5-68f1-482a-a405-ff993d8f4cb0
Timestamp: 2018-03-06T23:54:10Z
Message: Error AADSTSXXXX:
```

[Get resolution guidance](#)

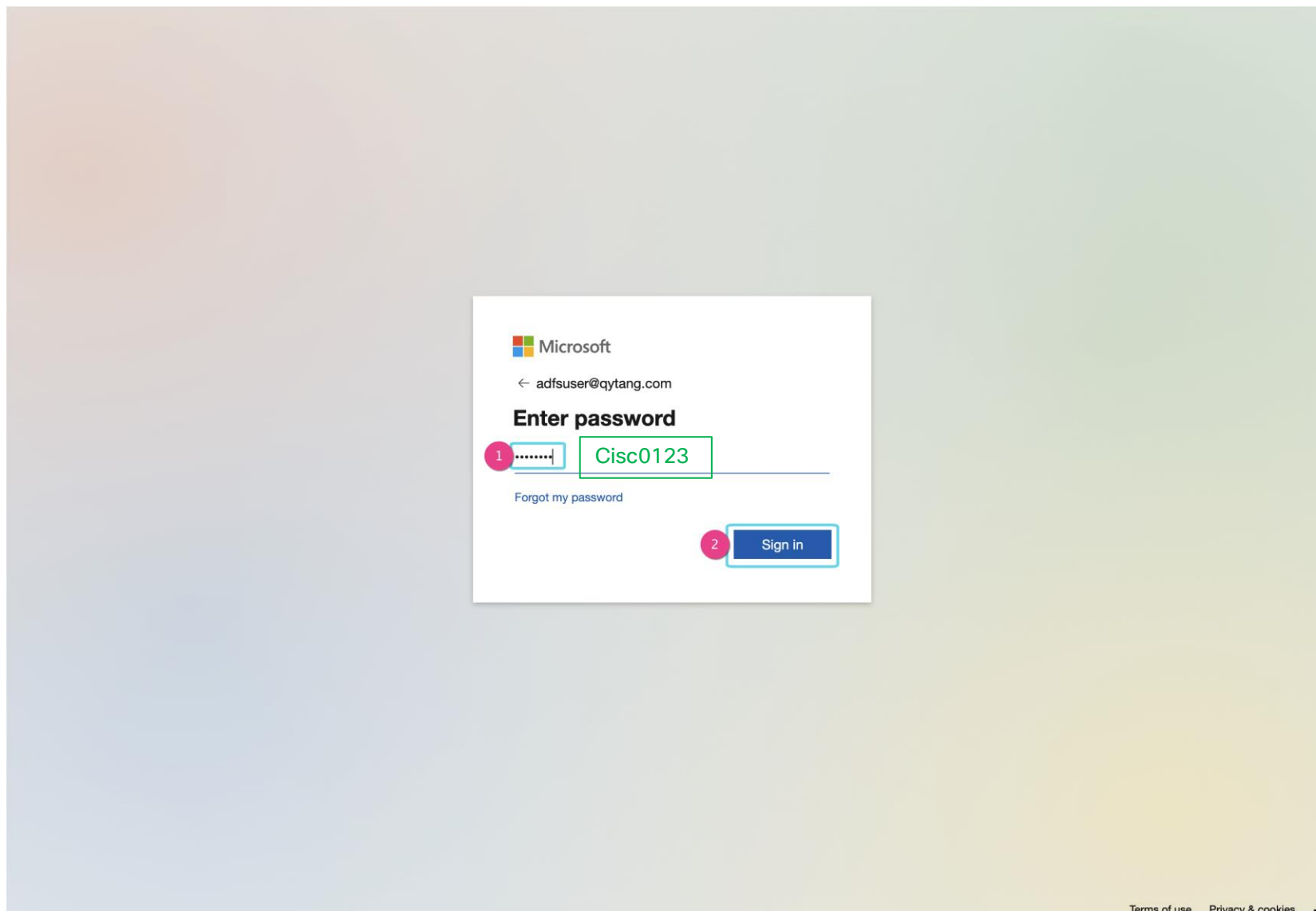


测试用户



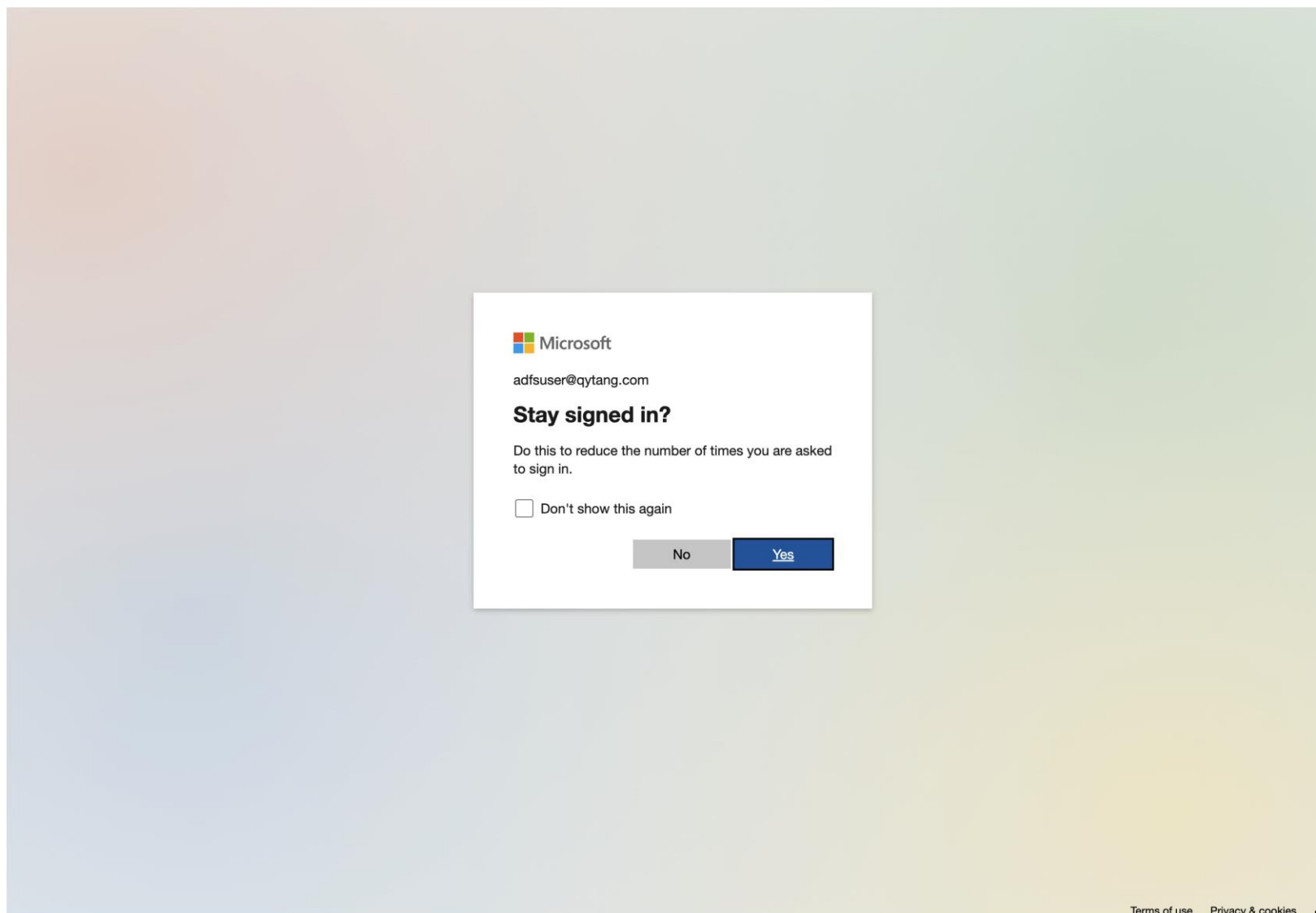


测试用户



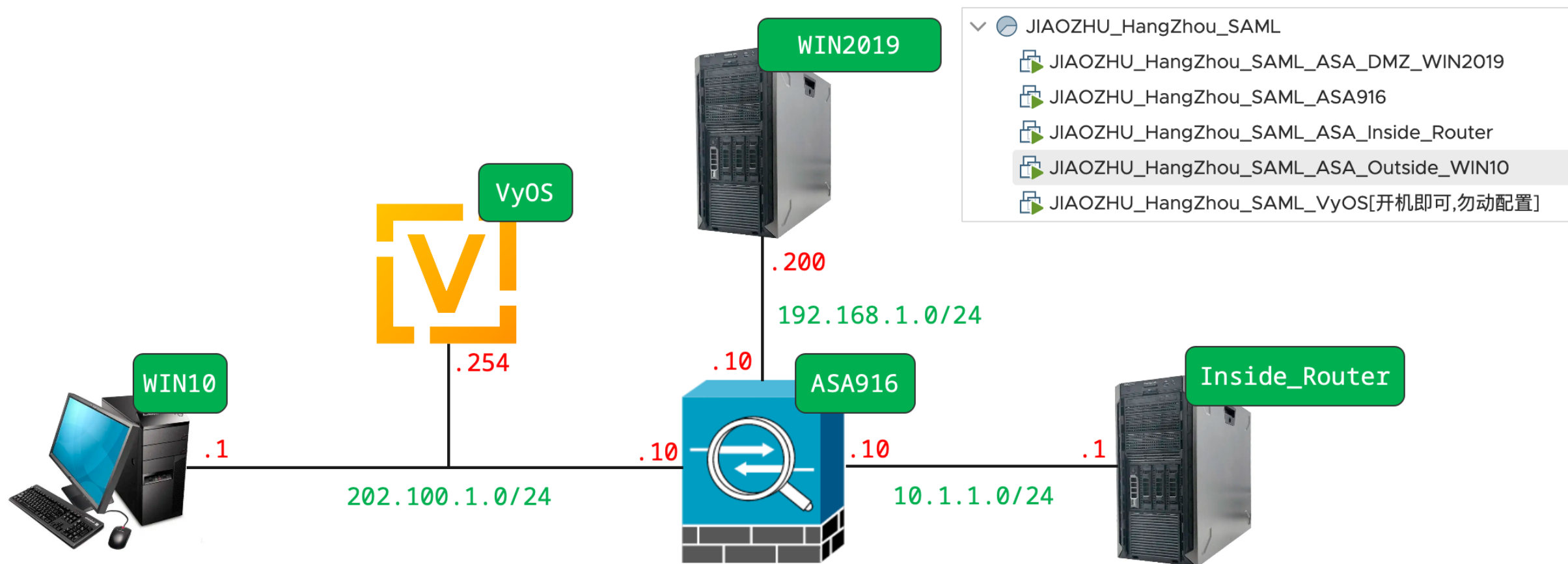


测试用户





实验拓扑





加载Azure证书

```
crypto ca trustpoint Azure-SAML
  revocation-check none
  no id-usage
  enrollment terminal
  no ca-check
```

```
crypto ca authenticate Azure-SAML
-----BEGIN CERTIFICATE-----
```

~~~下载的Cisco AnyConnect的证书~~~

```
-----END CERTIFICATE-----
```

```
quit
```

注意每次证书都不一样





# PFX文件转码到Base64

```
C:\Users\Administrator\Desktop\asa.qytang.com_iis\asa.qytang.com_iis>dir
```

驱动器 C 中的卷没有标签。  
卷的序列号是 ECEC-7DAD

```
C:\Users\Administrator\Desktop\asa.qytang.com_iis\asa.qytang.com_iis 的目录
```

```
2022/04/12 08:57 <DIR>      .
2022/04/12 08:57 <DIR>      ..
2022/04/11 09:36          4,670 asa.qytang.com.pfx
2022/04/11 09:36          250  该证书已设置私钥密码.txt
      2 个文件      11,344 字节
      2 个目录 191,016,157,184 可用字节
```

这是asa.qytang.com的ssl证书

```
C~~~>openssl base64 -in asa.qytang.com.pfx > asa.base64
```

把asa.qytang.com.pfx转码到  
base64



## 加载asa.qytang.com的ssl证书

```
ciscoasa(config)# crypto ca import QYTANG-SAML pkcs12 Cisc0123
```

Enter the base 64 encoded pkcs12.

End with the word "quit" on a line by itself:

~~~贴入base64编码后内容~~~

quit

文件位于 "桌面/asa.qytang.com_iis/asa.qytang.com_iis/asa.base64"



ASA基本网络配置

```
hostname ASA

interface GigabitEthernet0/0
 nameif Outside
 security-level 0
 ip address 202.100.1.10 255.255.255.0
!
interface GigabitEthernet0/1
 nameif Inside
 security-level 100
 ip address 10.1.1.10 255.255.255.0
!
route outside 0 0 202.100.1.254
```



ASA Webvpn配置

```
webvpn
enable outside
anyconnect image disk0:/anyconnect-win-4.10.05085-webdeploy-k9.pkg 1
anyconnect enable
tunnel-group-list enable
```

```
saml idp https://sts.windows.net/9a2af509-1e76-4091-9cbc-5286f5db8e7a/
url sign-in https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/saml2
url sign-out https://login.microsoftonline.com/9a2af509-1e76-4091-9cbc-5286f5db8e7a/saml2
```

Azure AD Identifier

Login URL

Logout URL

Azure证书

asa.qytang.com的ssl证书

asa.qytang.com是有效证书可以签名

```
base-url https://asa.qytang.com
trustpoint idp Azure-SAML
trustpoint sp QYTANG-SAML
signature rsa-sha256
no force re-authentication
```

```
ssl trust-point QYTANG-SAML outside
```



ASA LDAP配置

映射DN到Group Policy

```
ldap attribute-map qytang-ldap-map  
  map-name memberOf Group-Policy  
  map-value memberOf CN=adfs_group,OU=ADFS,DC=qytang,DC=com qytang-anyconnect  
  
aaa-server qytang-ldap protocol ldap  
aaa-server qytang-ldap (dmz) host 192.168.1.200  
  ldap-base-dn dc=qytang, dc=com  
  ldap-attribute-map qytang-ldap-map  
  ldap-login-dn cn=administrator, cn=users, dc=qytang, dc=com  
  ldap-login-password Cisc0123  
  ldap-naming-attribute sAMAccountName  
  ldap-scope subtree  
  server-type microsoft
```



ASA Tunnel-Group与Group-Policy配置

```
ip local pool qytang-pool 172.16.1.1-172.16.1.10 mask 255.255.255.0
```

```
group-policy qytang-anyconnect internal
group-policy qytang-anyconnect attributes
  banner value welcome to qytang saml
  dns-server value 192.168.1.200
  vpn-tunnel-protocol ssl-client ssl-clientless
  address-pools value qytang-pool
```

```
tunnel-group qytang-anyconnect type remote-access
tunnel-group qytang-anyconnect general-attributes
```

授权用LDAP

```
  authorization-server-group qytang-ldap
```

把后缀域名剥掉

```
  strip-realm
```

认证用SAML

```
tunnel-group qytang-anyconnect webvpn-attributes
```

```
  authentication saml
```

```
  group-alias QYTANG-SAML enable
```

```
  saml identity-provider https://sts.windows.net/9a2af509-1e76-4091-9cbc-5286f5db8e7a/
```

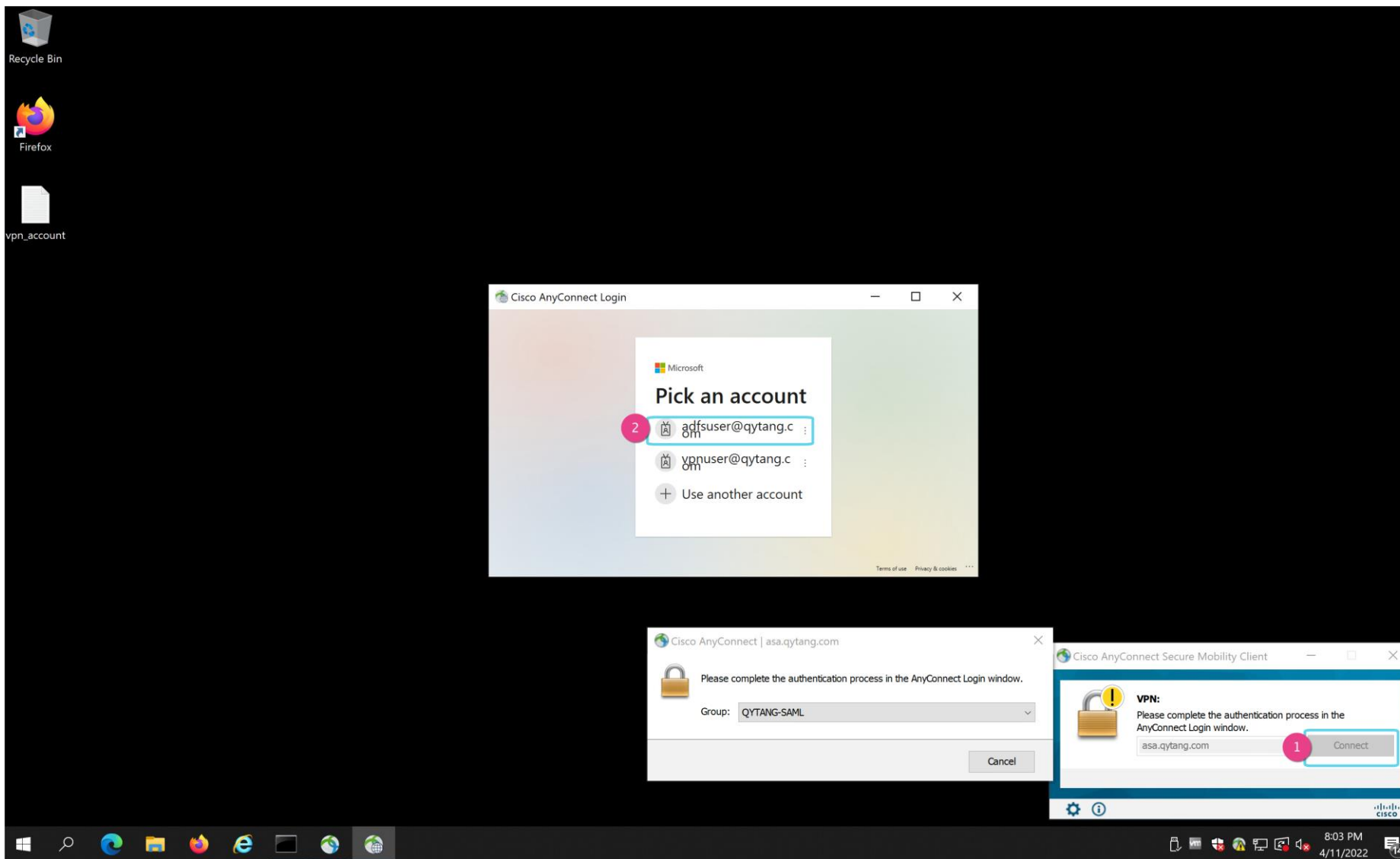
剥除前 adfsuser@qytang.com



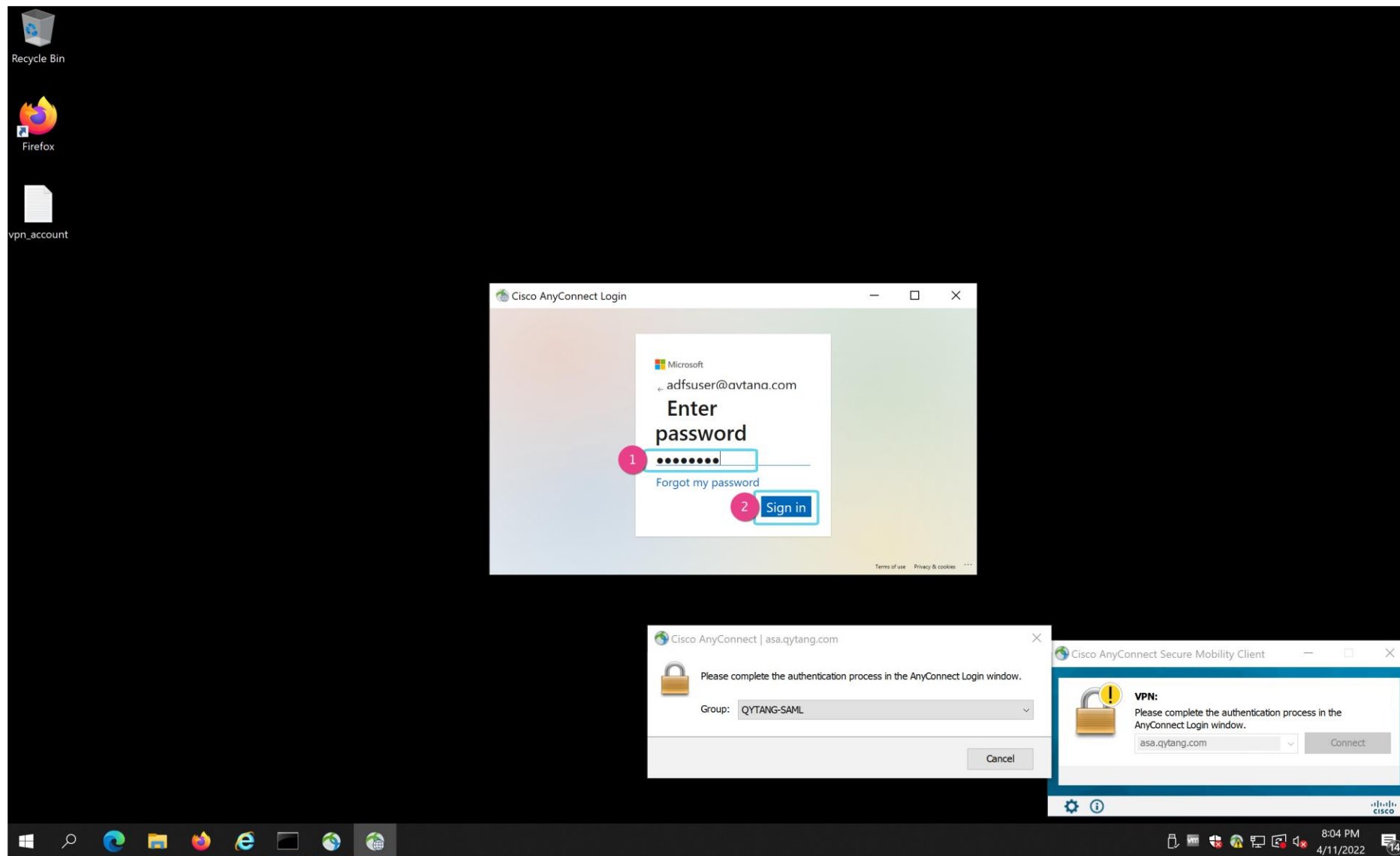
剥除后 adfsuser



WIN10 Anyconnect 测试

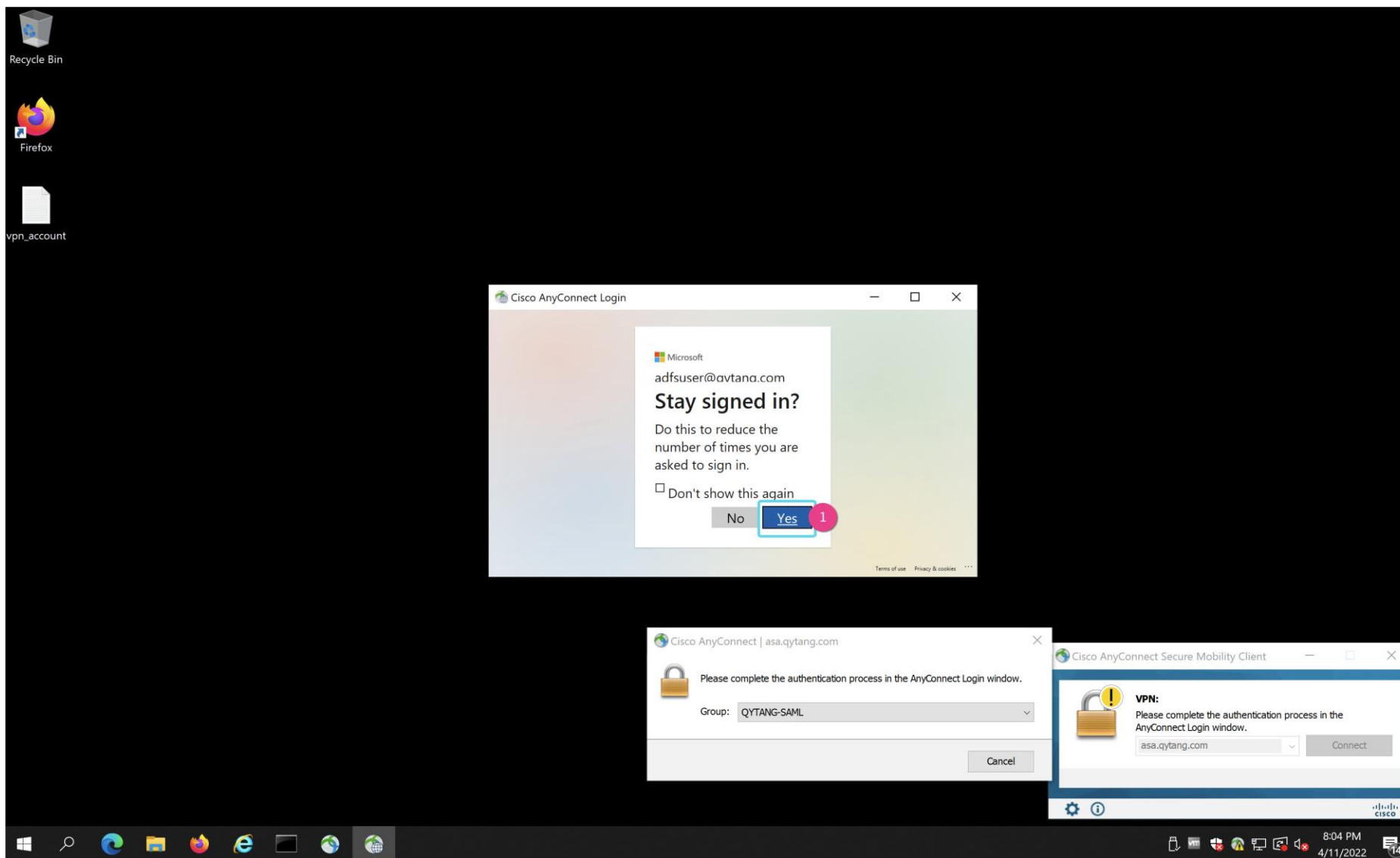


WIN10 Anyconnect 测试



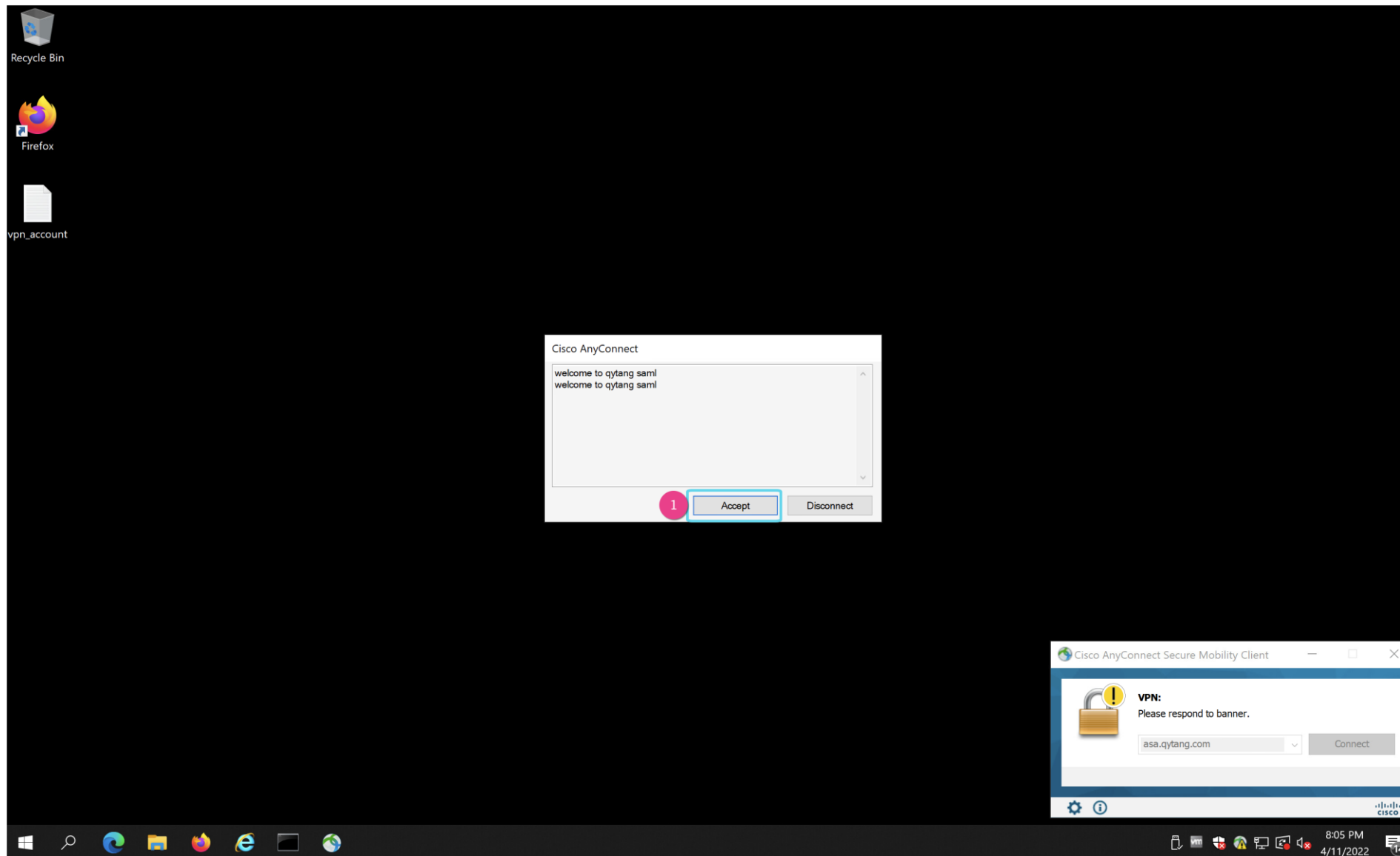


WIN10 Anyconnect 测试





WIN10 Anyconnect 测试





WIN10 Anyconnect 测试

The screenshot shows a Windows 10 desktop environment. On the left side of the taskbar, there are icons for Recycle Bin, Firefox, and a file named 'vpn_account'. The taskbar at the bottom includes the Start button, search icon, and several application icons. The system tray on the right shows the time as 8:06 PM and the date as 4/11/2022, along with network and volume icons.

```
Command Prompt
C:\Users\admin>ping 10.1.1.1

Pinging 10.1.1.1 with 32 bytes of data:
Reply from 10.1.1.1: bytes=32 time=2ms TTL=255
Reply from 10.1.1.1: bytes=32 time=11ms TTL=255
Reply from 10.1.1.1: bytes=32 time=2ms TTL=255
Reply from 10.1.1.1: bytes=32 time=2ms TTL=255

Ping statistics for 10.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 11ms, Average = 4ms

C:\Users\admin>
```