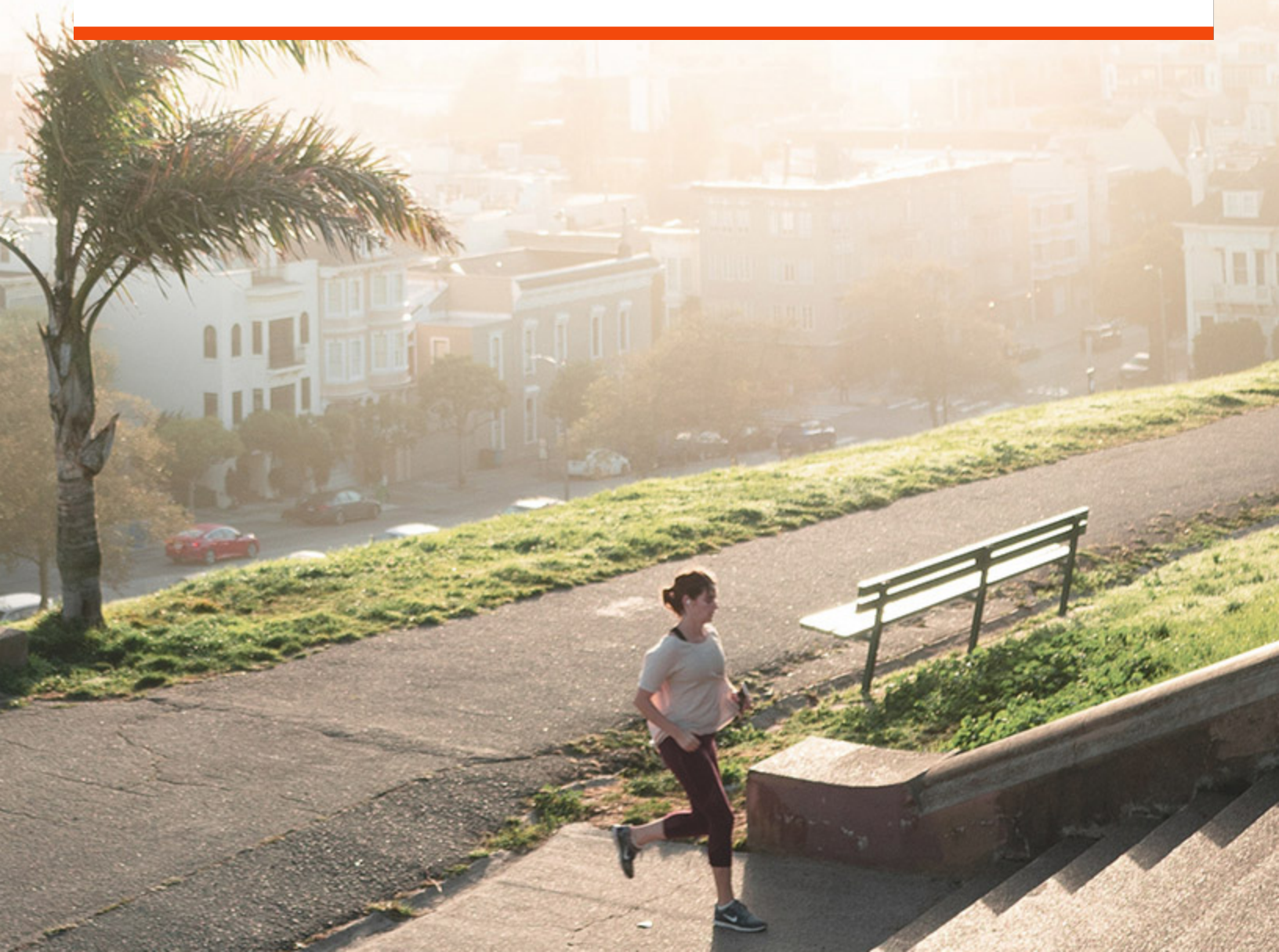


Community Development

MFA setup guide



Contact us

CentralSquare Technologies
1000 Business Center Drive
Lake Mary, Florida 32746
centralsquare.com

Customer portal and support

support.centralsquare.com • 833-278-7877 (833-CST-SUPP)

Education and training

csu@centralsquare.com • (800) 727-8088 • catalog.centralsquare.com • csu.litmos.com

Copyright © 2026. CentralSquare Technologies, LLC. All Rights Reserved.

Except as permitted under US Copyright Act of 1976, no part of this work may be reproduced, distributed, or transmitted in any form or by any means, or stored in a database or retrieval system, without prior written permission and consent of the publisher.

Community Development and Community Development's logo are trademarks of CentralSquare Technologies, LLC (herein "Publisher"), or its affiliates, successors, or assigns.

DISCLAIMER

All of Publisher's original works of authorship fixed in tangible mediums of expression, including but not limited to this publication of any associated software, are copyrighted under United States law and applicable international copyright laws and treaty provisions. The copyrights in the works are owned by the Publisher or by one of its affiliates, or by third parties who have licensed their materials to Publisher. The entire work of this publication, and any other copyrighted works of the Publisher, are copyrighted under United States law and applicable international copyright laws and treaties, and Publisher owns the copyright in the selection, coordination, arrangement and enhancement of said works. Publisher reserves all rights not expressly granted to the licensee.

You have been granted a limited non-exclusive license to use and/or access the published works under terms of the associated license agreement, and any other agreements governing the software listed on the cover of this publication; all of which are incorporated hereto.

Except as expressly stated in the applicable license agreement, you may not copy, download, print, publish, display, perform, distribute, transmit, transfer, translate, modify, add to, update, compile, abridge or in any other way transform or adapt all or any part of any of the Publisher's copyrighted works without first obtaining written permission from the Publisher.

No right, title, or interest in the copyrighted works is transferred to you when you access or use the works. Except for the limited, non-exclusive license expressly granted in the governing agreement, nothing contained in these terms and conditions shall be construed as conferring a license or ownership interest, be it by implication, estoppel or otherwise, or any other right under any copyright, trademark, patent, or other intellectual property right of Publisher or any third party.

The information in this copyrighted works is subject to change without notice.

In no event shall the Publisher be liable for any special, incidental, indirect, or consequential damages of any kind arising out of or in connection with the use of the Publisher's copyrighted works or other material derived thereof, whether or not advised of the possibility of damage, and on any theory of liability. This publication is provided "as-is." **The Publisher gives no express warranties, guarantees, or conditions. Publisher excludes all implied warranties and conditions, including those of merchantability, fitness for a particular purpose, and non-infringement. If local law does not allow the exclusion of implied warranties, then any implied warranties, guarantees, or conditions last only during the term of the limited warranty and are limited as much as local law allows. If local law requires a longer limited warranty term, despite this agreement, then that longer term will apply, but licensee can recover only the remedies allowed by the applicable governing agreement.**

Contents

MFA setup introduction	1
Preparing for MFA setup	1
Quick links	1
Find your path	2
Path A: Syncing on-premises Active Directory to Entra ID	2
Path B: You already use Microsoft 365 or Entra ID	3
Path C: Creating a free Entra ID tenant	3
Connecting Entra ID to Community Development	4
Step 1: Register the application	4
Step 2: Add the redirect URI	4
Step 3: Add the email claim	4
Step 4: Create a client secret	5
Step 5: Enter the values in Tenant Admin	5
Step 6: Set up Mobiles login in WUM (optional)	6
Step 7: Require MFA	6
Option A: Security defaults	6
Option B: Conditional Access (Entra ID P1 or P2)	6
Setting up your users	8
Contractors and external users	8
Login testing checklist	9
Reference	10
Tenant Admin access and responsibilities	10
Troubleshooting	10
Common questions	11
Meeting the November 13 deadline	11
Getting help	11

MFA setup introduction

This document details how to connect your identity provider and enable multifactor authentication (MFA) for Community Development.

Important: Action required: Complete by November 13, 2026. Your agency must connect a supported identity provider and enable multifactor authentication (MFA) before November 13, 2026. On that date, back-office login moves to your identity provider and local user names and passwords stop working. eTRAKiT, including the Citizen Portal and Agency Center, is not affected. November 15 is a Sunday, so plan to finish by Friday, November 13.

Target date	Milestone
Oct 23	Find your path.
Oct 30	Register Community Development in your provider and enter the values in Tenant Admin.
Nov 6	MFA is enabled, and every user and contractor has an account.
Nov 13	Login tested in staging, then production.
Nov 15	Enforcement begins.

Preparing for MFA setup

- **Client code:** It is the first part of your Community Development URL, <https://<CLIENTCODE>.csqrcloud.com>. If you cannot find it, open a case with CentralSquare Support.
- **Entra access:** You need a Global Administrator or Application Administrator account. Log in at <https://entra.microsoft.com>.
- **Identity Provider name:** Decide the exact name you will enter in Tenant Admin. It becomes part of the redirect URI, so use it the same way everywhere.
- **Tenant Admin access:** A Community Development administrator needs it. If a third party manages your accounts, send them this guide now.

Quick links

Link	Use
https://azure.microsoft.com/free	Create a free Azure account and Entra ID tenant (Path C)
https://github.com/microsoft/idfix	Check Active Directory before syncing (Path A)

Link	Use
https://learn.microsoft.com/en-us/azure/active-directory/hybrid/how-to-connect-install-roadmap	Download and install Entra Connect (Path A)
https://learn.microsoft.com/en-us/entra/fundamentals/security-defaults	Require MFA for free with security defaults
https://learn.microsoft.com/en-us/entra/external-id/add-users-administrator	Invite contractors as guests
https://www.microsoft.com/en-us/security/business/microsoft-entra-pricing	Entra ID plans and pricing

Find your path

CentralSquare does not offer a hosted MFA option that replaces this integration. Entra ID is the only provider with step-by-step instructions in this guide.

Your agency today	Go to	Effort
You have on-premises Active Directory (most ASPGOV-hosted agencies).	Path A : Sync to Entra ID, then connect it.	Medium, two to five days
You use Microsoft 365 or already have a Microsoft Entra ID tenant.	Path B : Go straight to connecting Entra ID.	Low, one to two days
You have no identity provider.	Path C : Create a free Entra ID tenant, then connect it.	Medium
You use Amazon Cognito, Okta, Duo, or another provider that supports OpenID Connect.	These can work, but this guide covers Entra ID only. Contact CentralSquare Support before you start. Path C is the fallback.	Contact Support now

Path A: Syncing on-premises Active Directory to Entra ID

Most ASPGOV-hosted agencies run Active Directory, so most start here. Entra ID has a free tier.

Effort: Two to five days. **Done when:** Your users appear under **Entra ID > Users**. If they already do, you are already syncing, so proceed to "[Connecting Entra ID to Community Development](#)."

1. Clean up your directory.
 - a. Run Microsoft IdFix to find duplicate proxyAddresses, invalid UPNs, and missing mail attributes.
 - b. Make each UPN match the user's real email domain.
 - c. Login names that end in .local cannot sync, so add your real email domain as a UPN suffix.
2. Prepare a server. Use a server that meets the following requirements:
 - Domain-joined Windows Server 2016 or later that is not a domain controller
 - At least 4 to 6 GB of RAM
 - 70 GB of disk
 - .NET 4.7.1 or later
 - TLS 1.2
3. Install Entra Connect.
 - a. In the Entra admin center, go to **Hybrid management > Microsoft Entra Connect**.
 - b. Download the installer.
 - c. Select **Password Hash Synchronization**.
 - d. Log in as a Hybrid Identity Administrator or Global Administrator for Entra, and as an Enterprise Admin for Active Directory.
 - e. Limit sync to the organizational units that contain Community Development users.
4. Verify the sync. Your users should appear under **Entra ID > Users** within about 30 minutes.

Path B: You already use Microsoft 365 or Entra ID

Your users are already in Entra ID. Continue to "[Connecting Entra ID to Community Development](#)."

Path C: Creating a free Entra ID tenant

Effort: Medium. **Cost:** \$0. **Done when:** Your users exist in the new tenant and security defaults are enabled.

1. Create a free Azure account at <https://azure.microsoft.com/free>. The account includes a free Entra ID tenant. Microsoft places a small card authorization and then reverses it.
2. Add and verify your agency domain under **Entra ID > Domain names**.
3. Create your users under **Users > New user**.
4. Confirm **security defaults** are enabled.

Connecting Entra ID to Community Development

Every agency completes this section.

Effort: One to two days. **Done when:** The app is registered, MFA is required, and the values are entered in Tenant Admin.

Step 1: Register the application

1. Go to **Entra ID > App registrations > New registration**.
2. Name the application "CentralSquare Community Development."
3. Select **Supported account types to Accounts in this organizational directory only**.
4. Select **Register**.
5. Copy the **Application (Client) ID** and **Directory (Tenant) ID**.

Step 2: Add the redirect URI

Redirect URI format: {base}/{clientcode}/signin/oidc/{clientcode}/{Identity Provider name, URL-encoded}

Staging base: https://sso.stg.csqrccloud.com

Production base: https://sso.csqrccloud.com

Spaces in the provider name appear as %20.

1. Go to **Authentication > Add a platform > Web**.
2. Enter the **Redirect URI**.
3. Select **ID tokens**.
4. Add one URI for staging and one for production.

CentralSquare Mobiles (optional): If you want Mobiles users to log in through your identity provider, also complete the following steps:

1. Go to **Authentication > Add a platform > Mobile and desktop applications**.
2. Select the **Custom redirect URI** option.
3. Enter **com.cstcomdev.mobile://auth**.

Step 3: Add the email claim

1. Go to **Token configuration > Add optional claim**.
2. Choose token type **ID**.

3. Select **Email**.
4. Go to **API permissions > Microsoft Graph > Delegated permissions**.
5. Add **Email** and **OpenID**.
6. Select **Grant admin consent**.

Step 4: Create a client secret

1. Go to **Certificates & secrets > New client secret**.
2. Copy the secret **Value**, not the **Secret ID**.
3. Record the expiration date.
4. Assign someone to renew the secret.
5. Set a calendar reminder at least 30 days before the expiration date to create a new secret and enter it in Tenant Admin.

When the secret expires, login stops.

Step 5: Enter the values in Tenant Admin

Enter the following values on the Identity Provider page in Tenant Admin:

Tenant Admin field	Value to provide
Name	The Identity Provider name you chose in " Preparing for MFA setup "
Client ID	The Application (client) ID from Step 1
Authority	https://login.microsoftonline.com/{tenant-id} , using the Directory (tenant) ID from Step 1
Secret	The client secret Value from Step 4
Response Type	code id_token
Identity Provider Vendor (staging only)	SelectEntra

CentralSquare does not need your client secret and should not receive it. If it has been shared with anyone outside your agency, complete the following steps:

1. Generate a new client secret in Entra ID.
2. Enter the new value in Tenant Admin.

Step 6: Set up Mobiles login in WUM (optional)

This step is optional. It lets Mobiles users log in through your identity provider, but Mobiles users can keep logging in as they do today. To enable it, complete the following steps:

1. In WUM, go to **System Settings > Login Security**.
2. In the **Mobiles Sign-In (OpenID Connect)** section, check **Allow users to sign in to Mobiles with the organization's identity provider**.
3. In the **Authority (identity provider URL)** field, enter the **Authority**.
4. In the **Client ID** field, enter the **Application (Client) ID** from [Step 1](#).

Step 7: Require MFA

Option A: Security defaults

This option is free.

Security defaults also block legacy login for IMAP, POP, and SMTP AUTH, so check scanners and service accounts first.

1. Go to **Entra ID > Overview > Properties > Manage security defaults**.
2. Set security defaults to **Enabled**.
3. Save your changes.
4. Revoke existing sessions so every user is prompted.

Users register Microsoft Authenticator the next time they log in, with no grace period.

Option B: Conditional Access (Entra ID P1 or P2)

This option is included in Microsoft 365 E3 and Business Premium, or refer to Microsoft for cost per user per month.

1. Disable security defaults.
2. Go to **Entra ID > Conditional Access > New policy**.
3. Include your Community Development users.
4. Exclude emergency access accounts.
5. Target the Community Development app.
6. Grant **Require multifactor authentication**.
7. Run the policy in **Report-only** first.
8. Switch the policy to **On**.

Note: If you completed [Path A](#), exclude the sync account from your MFA policies. Security defaults do this automatically. With **Conditional Access**, exclude the **Directory Synchronization Account**.

Setting up your users

Every agency completes this section, whichever path you took.

1. Add each user in Tenant Admin with an email address that exactly matches the email in Entra ID.
2. Assign roles to each user.
3. In WUM, go to **User Administration > OpenID Logins**.
4. Link the user's Community Development User ID to that email.
5. Wait up to 10 minutes for the cache to refresh before the user tests login.

After the switch, password resets happen in your identity provider, not in Tenant Admin.

Contractors and external users

Every contractor, consultant, and plan reviewer who logs in needs an account in your identity provider. To invite an external user, complete the following steps:

1. In Entra ID, go to **Users > New user > Invite external user**.
2. The guest(s) accept the invitation.
3. Add the guest(s) to Tenant Admin and WUM with the exact email on the invitation.

Guests are also required to complete MFA.

Login testing checklist

Staging is already enabled for some agencies. If your staging environment has identity provider details entered in Tenant Admin, staging sends you to that provider. If you cannot log in to staging, contact CentralSquare Support. Test in staging first, then production.

Before November 13, confirm the following:

- Your existing Community Development bookmark redirects to your identity provider login page.
- The MFA prompt appears and completes.
- The user lands in Community Development with the correct roles.
- A contractor or guest account can log in.
- You have recorded the client secret expiration date and assigned a renewal owner.

Reference

Tenant Admin access and responsibilities

If your agency already has a Tenant Admin administrator, that administrator can authorize and create additional users directly, and no case is needed.

If no administrator is available, open a case with CentralSquare Support titled "Tenant Admin access request" that includes the following information:

- Your agency name
- The environment (staging or production)
- The user's full name
- The user's email, exactly as it appears in your identity provider
- The access level needed

Task	Agency IT	Agency admin	Support
Register the app and require MFA in your identity provider.	A/R	I	I
Enter identity provider values in Tenant Admin.	C	R/A	I
Add users, roles, and OpenID Logins links.	C	R/A	C
Reset a password (managed in your identity provider).	R/A	C	I
Renew the client secret before it expires.	R/A	I	C

R = Responsible, A = Accountable, C = Consulted, I = Informed.

Troubleshooting

Symptom	Likely cause	Fix
Error AADSTS50011, redirect URI mismatch.	The URI in Entra ID does not match. This often happens after the provider name changes in Tenant Admin.	Copy the exact URI from the error message and add it to the application's redirect URIs.
Sign-in succeeds, then the user sees no access.	The email differs between your provider, Tenant Admin, and WUM, or the OpenID link is missing.	Correct the email and the link. Wait 10 minutes and retry.

Symptom	Likely cause	Fix
Remote login error.	The Client ID is wrong, or the client secret is wrong or expired.	Check the values. Create a new secret if needed and enter it in Tenant Admin.
No MFA prompt appears.	Security defaults or the Conditional Access policy is off, or the user is excluded.	Check the policy, then review Sign in logs > Conditional Access for the user.

Common questions

How do password resets work after this change?

Community Development passwords are managed in your identity provider. You reset them there, the same way you reset a Windows password for Active Directory, and not in Tenant Admin.

What is the process for adding a new user?

Add the user in your identity provider first. Then add the user in Tenant Admin and WUM, as described in "[Setting up your users](#)." This works the same way it does today for agencies already using single sign-on.

Does this affect EAUS, EPRS, or ECON users?

No. These online users are not affected.

Does this affect Agency Center or CentralSquare Mobiles?

Mobiles login through your identity provider is optional, and you can enable it in WUM ([Step 6](#)). Mobiles users can keep logging in as they do today. Agency Center is part of eTRAKiT and is not affected.

Meeting the November 13 deadline

Security threats are changing quickly, especially with the rise of AI, and from time to time CentralSquare and our customers need to act fast together to keep your environment secure. This is one of those times.

We ask every agency to do everything it can to finish by November 13. If you cannot meet the November 13 deadline, let CentralSquare Support know as soon as possible.

Getting help

- CentralSquare Support: 833.CST.SUPP (833.278.7877), or open a case on the CentralSquare support portal.
- [Tenant Admin User Guide](#)