Entra sync readiness check

City of Example (sample) · example.test

As of November 3, 2026

54

Work needed

Score out of 100

3 HIGH 4 MEDIUM 3 LOW

Checked 29 enabled user account(s) of 31 for what will break or change when this Active Directory starts syncing to Microsoft Entra ID (Microsoft 365). The Microsoft 365 tenant was included, so links to existing cloud accounts are predicted.

Staff list matching

11	3	2	2	0
Matched	Check	Multiple	Not found	Skipped

Rows that need a person to decide (first 40; the full list with every attribute is in matches.csv):

Row	Name in list	Status	Found	Why
9	TOD BREWER	Check	tbrewer (Todd Brewer)	Possible: first name differs
10	JOSH BENDOR	Check	jbendor (Joshua Bendor)	Possible: first name differs
11	CHRIS DAVIS	Multiple (2)	cdavis (Christopher Davis)	Possible: first name differs
11	CHRIS DAVIS	Multiple (2)	cdavis2 (Christine Davis)	Possible: first name differs
12	ADRIANNE GUITIERREZ	Check	agutierrez (Adrianne Gutierrez)	Possible: last name spelling
13	JESSICA VALENZUELA SANCHEZ	Multiple (2)	jvs1 (Jessica Valenzuela Sanchez)	Name
13	JESSICA VALENZUELA SANCHEZ	Multiple (2)	jvs2 (Jessica Valenzuela Sanchez)	Name
16	RAYMOND OKAFOR	Not found		
17	HELEN PRICHARD	Not found		

Cloud matching

HIGH **AD users would link to cloud accounts that hold admin roles; Microsoft blocks this**

Why it matters	Entra Connect is not allowed to link an AD user to a cloud account with an admin role (Existing Admin Role Conflict). That user fails to sync until it is fixed.
What to do	Keep admin accounts cloud-only and separate. Change the AD user's UPN and email aliases so they do not collide, or remove the role before the first sync and add it back after.
Found	• cloudadmin would link to cleo@example.gov, which holds an admin role

▶ How to fix it (about 15 minutes per account)

MEDIUM **People who would end up with two cloud accounts**

Why it matters	The AD account and the cloud account have the same name but neither the UPN nor the email address matches, so sync creates a second account instead of linking. The person loses access to their mailbox and files in the original account.
What to do	Before the first sync, make the AD user's UPN (or primary email alias) equal the cloud account's UPN so the two link.
Found	• ttran (ttran@example.test) and cloud account tina.tran@example.gov

▶ How to fix it (about 5 minutes per person)

INFO **What the first sync will do**

Why it matters	Check the new-account count against the number of people who already have Microsoft 365. If it is higher than expected, some people will get a second account.
What to do	Review matches.csv (when a staff list was supplied) and the duplicate-person and name-mismatch findings before turning sync on.
Found	• 1 will link to an existing cloud account • 26 will create a new cloud account • 1 already synced • 1 blocked (admin role) • 2 cloud-only account(s) no AD user will link to (they stay cloud-only)

Sign-in names

HIGH **Users sign in with an internal domain (such as .local) that Microsoft 365 cannot use**

Why it matters	Entra can only use verified internet domains. These users would sync with an onmicrosoft.com sign-in name instead, so their sign-in name changes without warning.
What to do	Add the company's email domain as a UPN suffix in AD, then change these users' UPNs to it (usually to match their email address) before turning on sync.
Found	• @example.local - 1 user(s), e.g. lortega • @example.test - 1 user(s), e.g. ttran

▶ How to fix it (about 30 minutes, plus user communication)

MEDIUM **Sign-in names Entra will reject or rewrite**

Why it matters	A UPN with a rejected character, an accent or too many characters is replaced with an onmicrosoft.com name when it syncs.
What to do	Correct each UPN in AD. The commands below suggest a cleaned-up value; confirm each one before running.
Found	• brian upton - brian upton@example.gov: contains a character Entra rejects

▶ How to fix it (about 2 minutes per user)

MEDIUM **Enabled users with no sign-in name (UPN) at all**

Why it matters	Usually old accounts created before UPNs were set. They sync with a generated onmicrosoft.com name, or are better left out of sync.
What to do	Give each person a UPN on your email domain (usually their email address), or exclude the account from sync if nobody uses it. Service accounts are listed under Accounts to keep out of sync.
Found	• nwhitfield

▶ How to fix it (about 2 minutes per user)

LOW **Users whose sign-in name differs from their email address**

Why it matters	People are told to sign in with their email address. When the UPN differs, sign-in fails or they call the help desk. It's also the most common reason two accounts fail to link.
What to do	Microsoft recommends the UPN match the primary email address. Change the UPN (preferred) or note the exceptions.
Found	• dprice - signs in as dprice@example.gov, email is shared@example.gov • dporter - signs in as dporter@example.gov, email is shared@example.gov • mmartinez - signs in as mmartinez@example.gov, email is mia.m@example.gov

▶ How to fix it (about 2 minutes per user)

Duplicates

HIGH **The same address belongs to more than one account**

Why it matters	Entra requires every UPN, mail and proxy address to be unique. The second account fails to sync (AttributeValueMustBeUnique) or links to the wrong cloud account.
What to do	For each address, decide which account should keep it and remove it from the others.
Found	• dandrews@example.gov - used by dandrews, preyes • shared@example.gov - used by dprice, dporter

▶ How to fix it (about 5 minutes per address)

MEDIUM **Email aliases (proxy addresses) Entra will reject**

Why it matters	An alias with a space, bracket or other rejected character stops that account from syncing.
What to do	Correct or remove each alias.
Found	• brian upton - brian upton@example.gov

▶ How to fix it (about 2 minutes per alias)

LOW **Mail nicknames that start with a period**

Why it matters	Entra rejects a mailNickname that starts with a period.
What to do	Remove the leading period.
Found	• dnichols - mailNickname '.dnichols'

▶ How to fix it (1 minute per user)

Sync scope

LOW **Accounts to keep out of sync**

Why it matters	Syncing unused, service and admin accounts adds cloud accounts nobody needs and gives attackers more to aim at. Microsoft recommends keeping admin accounts cloud-only.
What to do	Move these accounts into an OU that Entra Connect does not sync (OU filtering), or delete the ones nobody uses.
Found	• 2 disabled accounts; 1 enabled account with no sign-in for 90 days; 1 service account; 1 privileged (admin) account • Stale: skowalski • Service: svc_backup • Privileged: admin1

▶ How to fix it (about 1 hour)

What was read

Area	Result
User details	Read - 32 user object(s)

Read-only check. Nothing in Active Directory or Microsoft 365 was changed. AD Exit Planner 0.3.0.