Entra ID Integration with Google Workspace

SSO Implementation Guide for City of Calgary

1. Executive Summary

This document is prepared to explain how we are going to integrate Microsoft Entra ID (which was earlier called Azure AD) with Google Workspace for City of Calgary. The main purpose here is to make login process simple for users through Single Sign-On and to automate the user account creation and management.

What We Are Trying to Achieve

- We need to bring 20 suspended Google accounts under calgary.ca domain into proper management
- Users should be able to login with their Entra ID credentials only - no separate Google password needed
- When new employee joins or leaves, their Google account should automatically get created or disabled
- We will setup proper licensing for Cloud Identity Premium
- In future, some users may need Gemini access - we are keeping that in mind while designing

2. Current Situation and Problems

Before we start the implementation, let me explain what situation we are currently facing and why this project is important.

The Problems We Have Right Now

1. Unmanaged Accounts: There are 20 Google accounts under calgary.ca domain which are sitting suspended. Nobody is managing them properly.
2. Consumer State: These accounts are in consumer/unmanaged state. It means they were created by users themselves, not by IT department.
3. No Licensing: Organization does not have any Google Workspace licensing framework in place currently.
4. No Central Control: There is no centralized identity management connecting with Google Workspace.

What Is There Currently

- Domain: calgary.ca
- Identity Provider: Microsoft Entra ID - this is where all our users are managed
- Google Status: 20 accounts suspended, not managed by anyone
- User Count: 20 accounts that we need to migrate or consolidate

3. How The Solution Will Work

Let me explain the architecture in simple terms so that everyone can understand how different systems will talk to each other.

3.1 Overall Design

The basic idea is quite straightforward. When user wants to access Google services, they will be redirected to Entra ID for login. After successful authentication, they get access to Google Workspace. All user creation and updates will happen automatically through SCIM protocol.
Key Components:

- Entra ID: This is our identity provider. All authentication happens here.
- SAML 2.0: This protocol is used for SSO. When user logs in, SAML assertion is created and sent to Google.
- SCIM 2.0: This protocol handles automatic user provisioning. When we create user in Entra ID, it automatically gets created in Google Workspace also.
- Google Workspace: This is the service provider where users will access Gmail, Drive, and other Google services.

3.2 How Login Will Work (Step by Step)

1. User goes to Google service (like Gmail or Drive)
2. Google sees it is calgary.ca domain, so redirects user to Entra ID
3. User enters their normal City credentials and completes MFA if asked
4. Entra ID creates a SAML token saying "yes, this user is authentic"
5. User is redirected back to Google with this token
6. Google validates the token and gives access to the user

The whole process takes only few seconds and user does not even realize all this is happening in background.

3.3 How User Provisioning Works

Whenever there is any change in Entra ID - like new user joining, user leaving, or some attribute change - the provisioning engine picks it up and makes same changes in Google Workspace. This happens automatically every 40 minutes or we can trigger it manually if needed urgently.

4. Licensing Strategy

This section explains what licenses we need to buy and how we will assign them to users.

4.1 Which License To Use

We are recommending Cloud Identity Premium as the main license. Why this choice?
Because:

- We do not need productivity tools like Gmail inbox or Drive storage for most users
- Cloud Identity gives us enterprise-grade identity management
- It supports SAML SSO which is what we need
- Cost is much lower than full Google Workspace - around $6 per user per month
- Has good security features that enterprise needs

4.2 How To Assign Licenses

We suggest using Organizational Unit (OU) based licensing. In simple words, we will create different folders (OUs) in Google Admin Console and assign license to the folder. Any user put in that folder will automatically get that license.
Why OU-based is better:

- Very easy to manage - just move user to correct folder
- Follows natural organizational structure
- When new user joins, license gets assigned automatically
- This is how Google recommends to do it

Suggested OU Structure

- Cloud Identity Premium Users: For standard employees
- Gemini Enabled Users: For those who need AI features in future (will need Google Workspace Enterprise license)
- Service Accounts: For non-human accounts used by applications

5. Handling the 20 Unmanaged Accounts

This is important part of the project. We have 20 accounts that are currently in suspended, unmanaged state. We need to bring them under proper management.

5.1 First Step - Domain Verification

Before we can do anything with those accounts, we need to prove to Google that we own calgary.ca domain. This is done by adding special DNS records. Once verified, Google will recognize us as the legitimate owner.

5.2 Options for Handling Accounts

Option A - Account Transfer (Recommended if data is important)
In this approach, we contact Google Support and ask them to transfer those unmanaged accounts under our control. Users will keep their existing data - emails, files, everything. This is cleaner approach if users have important data in those accounts.
Option B - Delete and Recreate (Clean slate approach)
If data is not important, we can simply delete those accounts and create fresh ones through Entra ID provisioning. This is simpler but users will lose any existing data.

6. Implementation Plan

We have divided the implementation into 7 phases. This way we can do things step by step and catch any issues early.

Phase 1: Planning (Week 1-2)

- Audit all 20 unmanaged accounts
- Verify calgary.ca domain ownership
- Buy Cloud Identity Premium licenses
- Document current Entra ID user structure
- Design OU structure for Google Workspace

Phase 2: Google Workspace Setup (Week 2-3)

- Create Google Workspace Admin account
- Configure basic settings in Admin Console

- Create the OU structure as planned
- Consolidate the unmanaged accounts
- Assign licenses to OUs

Phase 3: SSO Configuration (Week 3-4)

- Configure Google Workspace as Service Provider
- Create Enterprise Application in Entra ID
- Set up SAML configuration and attribute mapping
- Test SSO with few pilot users
- Configure SSO enforcement policies

Phase 4: User Provisioning Setup (Week 4-5)

- Enable SCIM provisioning in Google Workspace
- Configure Entra ID provisioning connector
- Set up attribute mappings (email, name, department etc.)
- Test provisioning with pilot group

Phase 5: Pilot Testing (Week 5-6)

- Select 5-10 users from different departments for pilot
- Test complete flow - user creation, SSO, license assignment
- Test suspension and reactivation scenarios
- Collect feedback and fix any issues

Phase 6: Production Rollout (Week 6-8)

- Communicate to all users about the change
- Roll out in phases - IT first, then admin staff, then everyone else
- Enable SSO enforcement
- Provide training materials and help desk support

Phase 7: Post-Implementation (Week 8+)

- Monitor logs and fix any issues
- Document lessons learned
- Plan for future Gemini rollout
- Establish ongoing maintenance procedures

7. Technical Configuration Details

7.1 Entra ID Configuration

Here are the main steps for configuring Entra ID. The IT team should follow these carefully.

Creating Enterprise Application

1. Go to Entra ID Admin Center (entra.microsoft.com)
2. Navigate to Enterprise Applications and click New Application
3. Search for "Google Workspace" or "G Suite Connector by Microsoft"
4. Give it a name like "Google Workspace - City of Calgary"
5. Click Create

SAML Configuration

In Basic SAML Configuration:

- Entity ID: google.com/a/calgary.ca
- Reply URL: https://www.google.com/a/calgary.ca/acs
- Sign on URL: https://www.google.com/a/calgary.ca

7.2 Google Workspace Configuration

OU Structure

Create the following structure in Google Admin Console under Directory > Organizational Units:

- Corporate: For standard employees with Cloud Identity Premium
- Gemini Users: For those needing AI access (future)
- Contractors: For external contractors
- Service Accounts: For non-human accounts, SSO disabled

Attribute Mapping for Provisioning

These are the fields that will be synced from Entra ID to Google Workspace:

Entra ID Field	Google Workspace Field
userPrincipalName	primaryEmail
givenName	name.givenName
surname	name.familyName
department	organizations.department
jobTitle	organizations.title

8. Security Considerations

Security is very important in this project. Here are the key security measures we will implement.

8.1 Authentication Security

Entra ID Conditional Access Policies:

- Require MFA for all Google Workspace access
- Block access from unknown locations
- Require compliant device for access
- Block sign-in for high-risk users automatically

8.2 Data Protection

- Configure DLP rules to prevent sharing of sensitive data
- Enable SPF, DKIM, DMARC for email security
- Restrict external file sharing
- Enable audit logging with minimum 1 year retention

9. Contingency Plan - Break Glass Admin Accounts

This is very critical section. We must have a backup plan for situations when Entra ID is not working or SSO is broken. Otherwise, if something goes wrong with Entra ID, nobody will be able to access Google Workspace - not even administrators!

9.1 Why Break Glass Accounts Are Needed

Think about this scenario: It is Monday morning, everyone is trying to login to Google Workspace, but Entra ID is having issues. If all our admin accounts are also depending on Entra ID SSO, we cannot even go into Google Admin Console to disable SSO temporarily! This is very dangerous situation.
That is why we must create some admin accounts directly in Google Workspace that do NOT use Entra ID for login. These are called "break glass" accounts - like breaking glass to get fire extinguisher in emergency.

9.2 Break Glass Account Setup

Accounts to Create:
We recommend creating minimum 2 break glass super admin accounts. These accounts should be:

1. Created directly in Google Workspace Admin Console - NOT provisioned through Entra ID
2. Excluded from SSO enforcement - these accounts will use Google password, not Entra ID
3. Given Super Admin role - so they can make any configuration changes
4. Protected with strong security - long password + 2-Step Verification with hardware keys

Suggested Account Names:

- breakglass-admin1@calgary.ca
- breakglass-admin2@calgary.ca

9.3 Step-by-Step: Creating Break Glass Accounts

1. Login to Google Admin Console using existing admin credentials
2. Go to Directory > Users and click "Add new user"
3. Create the user with name like "Break Glass Admin 1" and email "breakglass-admin1@calgary.ca"
4. Set a very strong password - at least 20 characters with mix of everything
5. Assign Super Admin role under Account > Admin roles
6. Enable 2-Step Verification using hardware security key (like Yubikey)
7. Generate backup codes and store them securely
8. Move account to special OU where SSO is NOT enforced (create "Emergency Admins" OU with SSO disabled)
9. Repeat for second account

9.4 Storing Break Glass Credentials Securely

These credentials are like keys to the kingdom. They must be stored very securely.

- Physical Safe: Store password and backup codes in sealed envelope inside physical safe. Two different people should have safe combination.
- Password Manager: If using password manager, use one that is NOT dependent on Entra ID. Store in shared vault with very limited access.
- Hardware Keys: Keep the Yubikeys for 2FA in physical safe along with passwords. Keep spare keys in different location.

- Access Log: Maintain a register to track who accessed the break glass credentials and when.

9.5 When To Use Break Glass Accounts

Only use these accounts in real emergency situations:

- Entra ID is completely down and no administrator can login
- SSO configuration is broken and redirecting to wrong IdP
- SAML certificate has expired and needs immediate renewal
- Need to quickly disable SSO for troubleshooting
- Any other situation where Entra ID login is not possible but Google access is critical

9.6 Emergency Login Procedure

If Entra ID or SSO stops working, admin can login to Google Workspace using break glass account like this:

1. Go to admin.google.com (NOT google.com)
2. Click "Sign in with a different account" if SSO redirect happens
3. Enter break glass account email: breakglass-admin1@calgary.ca
4. Enter the password from secure storage
5. Complete 2FA using the hardware key or backup code
6. Once logged in, you can disable SSO temporarily or fix the configuration
7. After fixing, re-enable SSO and log out from break glass account

9.7 Regular Testing of Break Glass Accounts

It is no use having break glass accounts if they do not work when needed. We must test them regularly.

- Monthly: Verify that break glass accounts still exist and are active
- Quarterly: Actually login with break glass account to confirm credentials work
- Yearly: Change passwords and update stored credentials
- After any use: Immediately change password after any emergency use

9.8 Audit and Monitoring

All break glass account activity should be closely monitored:

- Set up email alerts in Google Admin Console for any login to break glass accounts
- Review Admin Audit logs weekly for any unexpected activity
- Any use of break glass account should be documented with reason and approved by IT Manager
- Conduct post-incident review after every emergency use

10. Disaster Recovery Procedures

Apart from break glass accounts, here are other recovery procedures to keep in mind.

10.1 If SSO Fails During Normal Operations

1. Login using break glass account
2. Go to Security > Authentication > SSO with third-party IdP
3. Temporarily disable SSO enforcement
4. Users can now login with Google passwords (if they have set them)
5. Communicate to users via alternate channel (email, phone, etc.)
6. Investigate and fix the SSO issue

7. Re-enable SSO after resolution

10.2 If Provisioning Stops Working

- New users can be created manually in Google Admin Console temporarily
- Document all manual changes so they can be reconciled later
- Check Entra ID provisioning logs for errors
- Re-sync accounts after provisioning is fixed

11. Monitoring and Maintenance

11.1 Daily Checks

- Review provisioning error logs in Entra ID
- Check for failed sign-in attempts
- Look at security alerts

11.2 Weekly Checks

- Review new user provisioning
- Validate license assignments
- Check for any suspended accounts

11.3 Monthly Checks

- Review access for all users
- Audit OU structure
- Check license utilization
- Test break glass accounts

12. Cost Estimation

Here is rough cost estimate for this implementation.

12.1 Licensing Costs

- Cloud Identity Premium: Around $6 USD per user per month
- For 20 users: Approximately $1,440 USD per year
- Google Workspace Enterprise (if Gemini needed later): Around $18-20 USD per user per month

12.2 Implementation Costs

- Contractor/Professional Services: $5,000-15,000 USD estimated
- Total Year 1: Approximately $6,440-16,440 USD

13. Common Problems and Solutions

User Cannot Login

1. Check if user is assigned to Google Workspace app in Entra ID
2. Verify user exists in Google Admin Console
3. Check if user's OU has SSO enabled

4. Look at Entra ID conditional access policies
5. Check if account is suspended
6. Verify SAML certificate has not expired

User Not Provisioned

- Check if user is in correct Entra ID group
- Review provisioning logs for errors
- Verify SCIM connection is working
- Check for duplicate email addresses

SSO Redirect Loop

- Clear browser cache and cookies
- Verify SAML URLs are correct
- Check NameID format configuration
- Validate certificate is not expired

14. Who Does What

City of Calgary IT Team

- Manage Entra ID and user groups
- Handle day-to-day support for users
- Monitor logs and respond to issues
- Maintain break glass account security

Contractor

- Help with domain verification
- Set up SSO and provisioning
- Consolidate unmanaged accounts
- Provide training and documentation
- 30-day support after go-live

15. Important Points to Remember

- Always keep break glass accounts ready - this is most critical for emergency situations
- Test break glass login procedure quarterly
- Store break glass credentials in secure physical location
- Follow the implementation phases - do not skip steps
- Monitor provisioning and SSO logs daily
- Keep documentation updated

Document Control

Version	Date	Author	Changes
1.0	[Date]	[Author Name]	Initial document

Classification: Internal Use Only
Review Schedule: Quarterly during implementation, Annually after go-live