Stage 4 focuses on testing and validating Azure AD connections to ensure the new authentication and access procedures are functioning effectively. This step is critical to securing VIP Events’ data and ensuring seamless integration with apps and services. The output of this stage includes detailed specifications for testing procedures.

**Task 1: Client App Integration**

To validate the integration of the VIP Food app with Azure AD:

1. Seamless Authentication:

- Test user login using Azure AD credentials to confirm that the app redirects users to Azure AD for authentication.

- Verify that after successful authentication, the app receives an authorization token and redirects the user back to the app via the configured redirect URI.

- Confirm that users can access the app without re-entering credentials (single sign-on).

2. Custom Role Utilization:

- Assign a test user to a custom role (e.g., `ChefsRole`) in Azure AD.

- Log in as the test user and verify that the app displays only the functionalities allowed for that role (e.g., kitchen management tools for chefs).

- Repeat the test for other roles (e.g., `EquipHandlersRole`, `OfficeRole`) to ensure role-based functionality is enforced.

**Task 2: User Account Validation**

To verify that all user accounts are correctly created and configured:

1. Account Creation:

- Check Azure AD to ensure all user accounts (e.g., Equipment Handlers, Chefs, CEO) have been created.

- Validate that user attributes (e.g., job title, department, email) are accurate and synchronized with the organization’s HR system.

2. Attribute Synchronization:

- Use Azure AD Connect to verify synchronization between on-premises directories (if applicable) and Azure AD.

- Confirm that attributes such as group memberships and custom claims are correctly updated.

**Task 3: Application Role Assignment**

To confirm role assignments and test access based on roles:

1. Role Assignment Verification:

- In Azure AD, check that each user is assigned to the correct custom role (e.g., `EquipHandlersRole` for equipment handlers).

- Ensure transient staff accounts are assigned temporary roles with expiration dates.

2. Access Testing:

- Log in as users from different roles (e.g., Chef, Office Worker) and attempt to access restricted resources.

- Confirm that users can access only the functionalities permitted by their roles (e.g., chefs accessing kitchen systems but not office systems).

**Task 4: Group/Role-Based Access Testing**

To validate role-based access control:

1. Access Granting:

- Test access to subnets and wireless segments (e.g., `Dock\_Operations`, `Kitchen`) by logging in as users from different groups.

- Verify that users can access only the resources relevant to their roles (e.g., equipment handlers accessing dock operations but not kitchen systems).

2. Access Restriction:

- Attempt to access restricted resources with unauthorized accounts (e.g., a guest user trying to access office systems).

- Confirm that access is denied and logged for auditing purposes.

**Task 5: MFA Verification**

To validate multi-factor authentication (MFA):

1. MFA Configuration:

- Enable MFA for all user accounts in Azure AD.

- Test MFA by logging in as a user and verifying that the second authentication factor (e.g., Microsoft Authenticator app or SMS code) is required.

2. Privileged Accounts:

- Ensure MFA is enforced for privileged accounts (e.g., CEO, Equipment Manager).

- Test scenarios where MFA fails (e.g., incorrect code) to confirm access is denied.

**Task 6: Logging and Monitoring**

To validate logging and monitoring:

1. Azure AD Logs:

- Navigate to Azure AD > Monitoring > Sign-ins to view logs of successful and failed sign-in attempts.

- Check logs for role assignments, changes in user attributes, and other administrative activities.

2. Testing Logs:

- Simulate various scenarios (e.g., successful login, failed MFA, role changes) and verify that these activities are captured in the logs.

- Test log retention settings to ensure compliance with organizational policies.

**Task 7: Documentation Review**

To cross-verify Azure AD configuration documentation:

- Alignment with Requirements:

- Compare the actual Azure AD setup with the documented requirements from previous stages.

- Ensure all configurations (e.g., custom roles, MFA, redirect URIs) are accurately documented.

- Screenshots:

- Capture screenshots from the Azure portal (e.g., role assignments, user attributes, logs) to supplement the documentation.

**Documentation Summary**

Add the testing strategy created in this stage to your proposal. Include:

Test Procedures:

- Detailed steps for validating app integration, user accounts, role assignments, and access control.

- Results:

- Document the outcomes of each test, including any issues encountered and resolutions applied.

- Screenshots:

- Provide visual evidence from the Azure portal to support the documentation.

This testing strategy ensures VIP Events has a comprehensive reference for validating Azure AD connections and maintaining a secure environment.