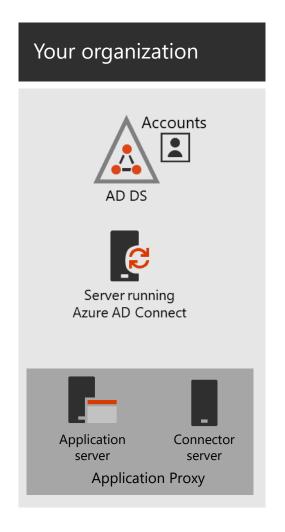
# Empower remote workers with Microsoft 365 for enterprise

A combination of features in Microsoft 365 for enterprise enables your workers to work from anywhere and at any time in a highly collaborative, productive, and secure way.



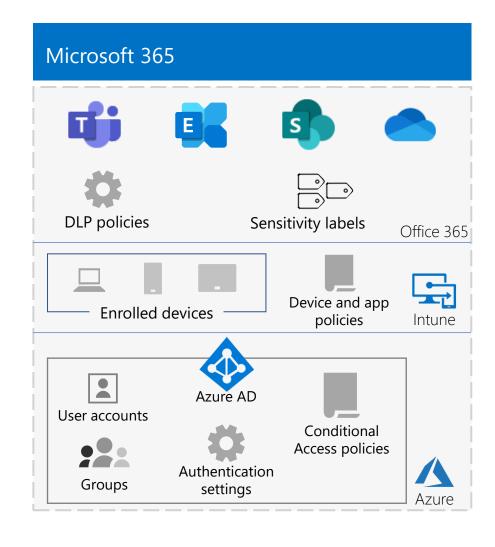
### Remote worker architecture and configuration





Windows 10

Enterprise device





Data Loss Prevention (DLP)
Policies to prevent leakage of
highly regulated data



Sensitivity labels for encryption and permissions that travel with files

#### Intune



Device enrollment to receive features and security settings and device and app policies



Device and app policies to allow or block apps and detect non-compliant devices

# e Azure AD



User accounts, either created in Azure AD or synced from AD DS



Office 365 and Azure Active Directory (Azure AD) security groups to assign policies and permissions



Authentication settings to require multi-factor authentication (MFA)



Conditional Access policies to block clients that don't support modern authentication

### Remote worker with a Windows 10 Enterprise device



- Remote worker:
- User account
- MFA sign-in
- Group membership
- Windows 10 Enterprise device:
- Office 365 ProPlus installed
- Joined to AD DS and Azure AD
- Enrolled in Intune
- Security features enabled

## Rolling out remote working in your organization

#### Phase 1: Deploy

- Configure identity infrastructure for users, groups, and authentication settings
- Deploy Windows 10 Enterprise to Windows devices
- Install Office 365 ProPlus on Windows, iOS, and Android devices
- Deploy Intune device and app management and enroll devices
- Configure DLP policies and sensitivity labels

## Phase 2: Drive user adoption

- Train remote workers on:
  - Sign-in with MFA
- Device use and allowed apps
- Windows 10 Enterprise security features
- Outlook, Teams, SharePoint, and OneDrive
- Using sensitivity labels
- Review remote worker usage and address feedback
- Retrain as needed