MSP Best Practices (Pax8)

Below you will find best practices gathered from the MSP community.

1. Use custom groups to enable the creation of a support team or tiered structure that aligns with the MSP business needs. Consider creating a role structure based on the different tiers of an MSP Technician. Or create separate groups for your onboarding team vs your support/help desk teams.
2. Add at least 1 additional account to the Owners group in the MSP Console.
3. If an MSP is co-managing with a managed company; Add at least 1 additional account to the Owners group in the managed company.
4. If an MSP is co-managing with a managed company; Owners/Administrators can recover accounts, consider creating a custom group to give additional members permission to recover accounts.
5. Set up a multifactor authentication method in your MSP account. These are required in MSP accounts in order to perform sensitive actions like launching into a managed account.
6. Consider enforcing additional security policies in your MSP account, such as strong password requirements, to ensure the security of your own company and all of your managed companies.
7. Configure integrations and automations in your MSP account & managed accounts to streamline your operations:
    a. Slack integration to manage notifications
    b. SIEM tool integrations for security monitoring
    c. Use the 1Password development tools to create automate your workflows
8. Integrate SCIM with your identity provider for automated provisioning and de-provisioning.
9. To develop your internal guidelines on selling, deploying and supporting 1Password access the latest resources in the 1Password Vendor Profile.
10. Review the Customer Best Practices support article for additional best practices.

If you have additional best practices, please share them through our feedback form to help strengthen our MSP community.