

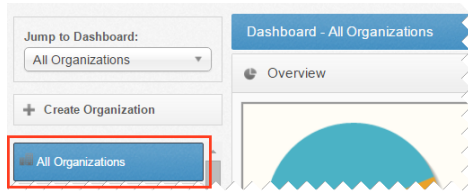
BEST PRACTICES FOR ANCHOR ADMINISTRATORS

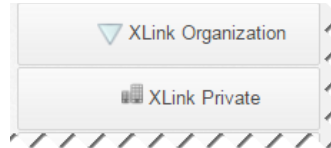
Welcome to eFolder! We are excited to help you get started as an Anchor administrator. This summary guide highlights important best practices to guide you as you create and manage organizations and support end users.

How can I use this document?

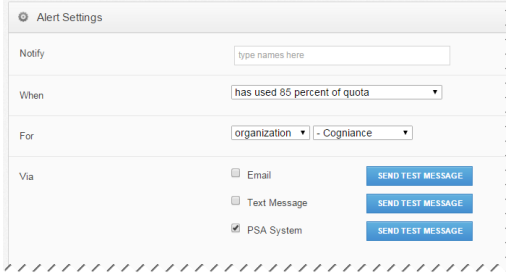
This document should be used in conjunction with the eFolder Knowledgebase, as well as Anchor administrator guides. The table below indicates where you can find additional information to better understand each best practice.

What best practices should I know before I get started?

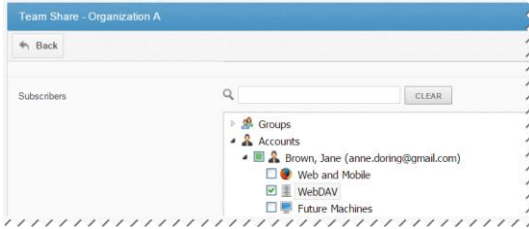
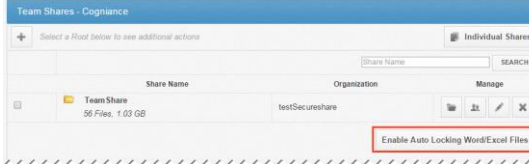
| Best practice | What it means | Why it's important | Where you can find more information |
|---|---|---|--|
| 1. Limit access to the master organization | <p>When you first log in to the administrative web portal, you will only see one organization in the left-hand Organization navigation bar. This is the master organization.</p>  <p>This master organization should remain <i>empty</i>; except for a few trusted administrators, users should not be given access to the master organization, and it should never be configured for internal or customer use.</p> | <p>Organization administrators have the ability to view content and user account information within the organization to which they have been assigned. Additionally, unless Privacy Mode has been enabled, they also have the ability to view this information in lower-level organizations. To mitigate the chance of exposing sensitive customer data to unauthorized individuals, you should only create organization administrator users within the organization to which they <i>need</i> access.</p> <p>Additionally, the master organization's Dashboard provides a totaled overview of all organization data usage, activity, and so forth. If the master organization is actively used as an organization, there is no way to view the actual usage for this</p> | <p>How Do I Use the Administrative Interface</p> |

| | | | |
|--|---|--|---|
| | | organization apart from suborganizations' usage. | |
| 2. Take advantage of the relationship between organizations and suborganizations | <p>When you create a suborganization, it inherits certain policies from its parent; you can also configure separate policies while still allowing the two entities to maintain a relationship and share resources.</p> <p>For example:</p> <ul style="list-style-type: none"> In general, it is recommended that you keep the <i>Allow users to erase deleted files</i> policy turned off; however, if one or two users need to retain this privilege, create a suborganization, turn on this policy in the new suborganization, and add these users to the suborganization. If you want to turn on Privacy Mode for one or two users (for example, a CEO), create a suborganization, add this user, and then turn on Privacy Mode (see below for best practices related to Privacy Mode). If you want to restrict storage quota for a Team Share, create a suborganization for this Team Share, and configure storage quota policies accordingly. | <p>You can take advantage of the system's flexible, multi-tenant structure to make the best use of policies and settings.</p>  <p>Please note, however, that if you reorganize organizations and suborganizations after File Server Enablement is mapped to a Team Share, these mappings might break when moving the Team Share. Please contact eFolder Support for help.</p> | <p>How Do I Manage Inherited Policies in Suborganizations</p> <p>How Do I Create and Configure Policies</p> |

| | | | |
|--|---|---|--|
| <p>3. Configure branding, outbound email, and email templates before deploying agents</p> | <p>If you decide to utilize custom branding settings, or if you would like to set up your own email settings for outbound emails (for sending alerts, welcome messages, and so forth), this should be done prior to inviting users and deploying agents.</p> | <p>If an end user installs an agent before branding is configured, the agent will not reflect these new branding settings. Agents need to be reinstalled to reflect new branding settings.</p> <p>Additionally, properly setting up an email settings for an organization will ensure that end users receive email notifications.</p> | <p>How Do I Configure Custom Branding</p> <p>How Can I Update Agents with New Branding Setting</p> <p>How Do I Set Up Microsoft Exchange to Work with Anchor</p> <p>How Do I Customize Email Templates</p> |
| <p>4. Take advantage of integration options</p> | <p>You can integrate Anchor with various technologies.</p> <ul style="list-style-type: none"> • To improve bounce rates for outbound emails, integrate with your preferred email system (including Microsoft Exchange, Office 365, Gmail, and more). • To import user accounts, integrate with any LDAP authentication source (for example, Active Directory). • To easily manage customer alerts, integrate with a PSA system (including ConnectWise and Autotask); these should be set up in conjunction with alerts. • To track collisions, integrate with a RMM platform (for example, LabTech); you can then configure | <p>These integration options will help you support and manage your customers.</p> <p>You can also utilize our API for customized integration options.</p> | <p>How Do I Set Up Microsoft Exchange to Work with Anchor</p> <p>How Do I Set Up Active Directory with Anchor</p> <p>How Do I Integrate Anchor with ConnectWise</p> <p>How Do I Integrate Anchor with Autotask</p> <p>How Do I Track Collisions in Anchor</p> <p>How Do I Work with the Anchor API</p> <p>How Do I Work with Anchor API v2</p> |

| | | | |
|--|---|---|---|
| | rules through your RMM platform. | | |
| 5. Allocate sufficient storage quota | <p>It is important to allocate sufficient storage in a way that accounts for growth and data retention. You should consider that Team Shares, personal files and folders, deleted files and folders, revisions, and backups all consume data. Note that Team Share deletions and revisions will count towards storage quota of the Team Share.</p> <p>User accounts can be configured to consume this data in one of two ways:</p> <ul style="list-style-type: none"> • Shared quota—this option allows the user as much storage as necessary, up to the organization limit. In most cases, you will probably utilize this option. • Individual space quota—this option allows the user a fixed storage limit. This is useful in specific instances, like when one user consumes a lot of data, and needs to be restricted. | <p>When the data quota has been reached for a user account or for the organization, the sync process might be affected.</p> <p>To help track storage quota, it is recommended that you create an alert in the <i>Activity</i> tab to be notified when an organization—or a user account—has reached a certain percentage of its storage quota.</p>  <p>You might also consider integrating with a PSA system, or creating an email rule, to track and manage these alerts. Finally, use the <i>Reports</i> tab to create reports that will help you track storage usage within the system.</p> | <p>How Do I Determine Space Quota Limits for Organizations</p> <p>How Do I Manage the Anchor Activity Log</p> |
| 6. Pay attention to bandwidth throttling | Anchor's bandwidth throttling feature allows you to conserve resources used by one machine, or one organization, in order to allow other machines to transfer data more efficiently when the server or | The agent utilizes all available bandwidth, unless otherwise restricted at the organization level or the individual machine level. Bandwidth throttling settings allow administrators to specify a maximum amount of data (in Kilobytes) | How Do I Configure Anchor Bandwidth Throttling |

| | | | |
|---|--|---|--|
| | <p>agent location has limited bandwidth.</p> <p>As an administrator, you can configure bandwidth throttling settings at the organization level, or for individual machines.</p> <p>Additionally, end users can each configure individual bandwidth settings through the agent's <i>Properties</i> dialog box.</p> | <p>to transfer per second; these settings are not configured based on a percentage of available bandwidth. If the server sends a block of data, the network will send it as quickly as possible. When download or upload speeds hit the maximum bandwidth setting, the speed is throttled back before the next block of data is sent</p> <p>Bandwidth throttling settings should be considered based on specific environment and network variables, so it is important to understand how bandwidth throttling works before making changes to an organization or a machine policy. When configuring server-side bandwidth throttling settings, for example, you should monitor the server to ensure that bandwidth is not restricted to a point that might cause collisions.</p> | |
| <p>7. Create dummy accounts when configuring File Server Enablement and Active Directory</p> | <p>When you need to install and register an agent on a server—for example, for File Server Enablement or Active Directory integration—register the agent to a dummy account, rather than a real account used by a real user.</p> <p>A dummy account should not be subscribed to Team Shares or contain personal files and folders, should be set to use a fixed space quota of .01GB, and should be configured using a predetermined</p> | <p>Using a dummy account will prevent unnecessary storage usage.</p> <p>You have two options to help you manage dummy accounts:</p> <ul style="list-style-type: none"> • Create one dummy account in the master organization, and register all File Server Enablement and server agents to this one dummy account. • Create one dummy account for each organization. | <p>How Do I Manually Create User Accounts</p> <p>How to Cloud Enable a Server Using File Server Enablement</p> |

| | | | |
|---|---|---|---|
| | naming system (such as First Name: File Server; Last Name: LDAP). | | |
| 8. Plan Team Shares to take advantage of subscription rules | <p>You can use subscription rules to control whether or not Team Share content is synchronized to certain devices. You can select from the following subscription rules:</p> <ul style="list-style-type: none"> • Web and mobile access • WebDAV access • Machine (agent) access <p>To best utilize these subscription rules, create separate Team Shares for content that should only exist on certain device types.</p> <p>Additionally, in the <i>Shares</i> tab of the end user web portal, end users can also turn off the syncing of Team Share content to their machine (agents).</p> | <p>Team Share subscription rules are useful when you want to prevent certain Team Share content—for example, a Team Share with large video files—from utilizing local storage on users' machines.</p> <p>For example, you can use subscription rules that ensure Team Shares with large file types don't sync down to machines, and instead only display in the web portal or through WebDAV.</p>  | <p>What is a Team Share</p> <p>How Do End Users Share Content</p> |
| 9. Configure Auto Locking and hard locks for Team Shares | <p>In most instances, it is recommended that administrators turn on the <i>Auto Lock Word/Excel</i> feature for Team Shares, and also enable hard locks.</p> <ul style="list-style-type: none"> • The <i>Auto Lock Word/Excel</i> feature automatically prompts users to lock Microsoft Word and Excel files each time they are opened. | <p>By turning on the <i>Auto Lock Word/Excel</i> feature for Team Shares, and by enabling hard locks, you ensure the best possible user experience and help prevent file sync conflicts.</p>  | <p>What is a Team Share</p> <p>How Do I Manage the File and Folder Locking Feature</p> <p>How Do End Users Lock Files and Folders</p> |

| | | | |
|--|--|--|---|
| | <ul style="list-style-type: none"> The <i>Use Filesystem Permissions</i> policy determines whether locks are <i>hard</i> or <i>soft</i>. <p><i>Hard locks</i> change the NTFS permissions on Windows, or HFS Plus permissions on Mac, in order to prevent users from editing a locked file.</p> | | |
| 10. When transferring large amounts of data to the Anchor server, take advantage of File Server Enablement | <p>When you turn on File Server Enablement for a machine, you can easily sync that data to a Team Share that already exists on the Anchor server.</p> <p>To facilitate the transfer of a large data set to the Anchor server, you can turn on File Server Enablement for multiple VMs, rather than rely on one server to transfer this data.</p> | <p>When you make use of multiple VMs—rather than just one single server—you can reduce the amount of time it takes to transfer data.</p> <p>For example, if transferring 1TB of data from one machine takes one month, transferring this data from two machines will take two weeks.</p> | How to Cloud Enable a Server Using File Server Enablement |
| 11. When troubleshooting syncing issues, refer to machine logs as a first step | <p>If you suspect that the system is not properly syncing data, you can monitor the syncing process in a number of different ways:</p> <ul style="list-style-type: none"> View logs in the <i>Machines</i> tab. Compare the number of files in Team Shares with the number of files in any mapped file server. | <p>You can often troubleshoot and diagnose syncing problems by reviewing these logs and database files.</p> <p>If you do find sync issues, ensure that the version of any affected agent is current. You might also try stopping and restarting the service on an affected machine.</p> <p>It is recommended that you <i>never</i> uninstall and reinstall the Anchor agent.</p> <p>If you uncover major issues, please contact eFolder Support.</p> | How to Capture Sync Agent Logs with Advanced Filtering on Windows Machines How to Retrieve Logs from the Mac Agent |

| | | | |
|---|---|---|---|
| <p>12. If applicable, turn on Privacy Mode as a last step</p> | <p>If you decide to turn on Privacy Mode for an organization, ensure that this feature is turned on as a last step. Specifically, before you turn on Privacy Mode, make sure that:</p> <ul style="list-style-type: none"> • Team Shares are created • User accounts have been created and added to Team Shares • File Server Enablement is configured • An alert has been created in the <i>Activity</i> tab to notify when an account has been added to the organization, or when a user has been subscribed to a Team Share | <p>When Privacy Mode is enabled for a lower-level organization, you will not be able to:</p> <ul style="list-style-type: none"> • Browse or manage the content of personal folders, team shares, or backups • Create backups • Subscribe to team shares • Move items—such as user accounts or team shares— to outside organizations • Configure File Server Enablement <p>You should create alerts to ensure that only authorized users have access to the organization.</p> | <p>How Do I Use the Anchor Privacy Mode feature</p> |
|---|---|---|---|



The People Behind Your Cloud