BEYOND IDENTITY

Implementing Beyond Identity: Frequently Asked Questions

We receive questions from new customers about the implementation process and so we assembled the most common questions with answers below.

Q: What policies do you recommend?

A: At a minimum, your security policy should check for and block any connections from modified mobile devices (referred to as "jailbroken" for iOS, and "rooted" for Android devices). For desktop users, you should require users to have antivirus software installed and a firewall active, and users should also enable hard drive encryption.

Enterprise deployments are far more complex and require more granular security policies, and what will be necessary varies based on your current security posture. In these situations, we work with your security and identity access management team(s) to determine the appropriate policies for your implementation. This process may take up to 90 days to complete.

We will look at the following factors when deciding on the best policies for a new enterprise installation:

- MDM enrollment (Jamf, Intune, etc.)
- Endpoint security software
- Zero trust score
- Domain join status
- App criticality
- Filepath
- Registry key

Q: What's the fastest way to roll out Beyond Identity?

A: While the actual process of integrating Beyond Identity with many common single-sign-on platforms is quite simple, there's a lot more to transition to more secure authentication. Our experience indicates it takes about 90 days to develop, test, and implement our platform from start to finish.

If you've already started transitioning to a zero trust security architecture before considering Beyond Identity, your implementation time will be far quicker than those who may be starting from scratch. In any case, our support teams will provide recommendations and assistance throughout the process.

When you're ready to roll out our platform to your end users, our customers generally do this in either of two ways:

- With MDM: The admin creates a user group policy to download Beyond Identity's app onto employee devices in the organization's MDM. The admin e-mails the organization to open the app and register for a credential.
- Without MDM: Organizations not using MDM can e-mail the organization and have them download and install Beyond Identity's app on their own.

Q: Who are my points of contact throughout onboarding and beyond?

A: We will introduce you to all the necessary contact points during your kickoff call. Your customer success manager will schedule this call and be your primary point of contact for anything you need regarding Beyond Identity.

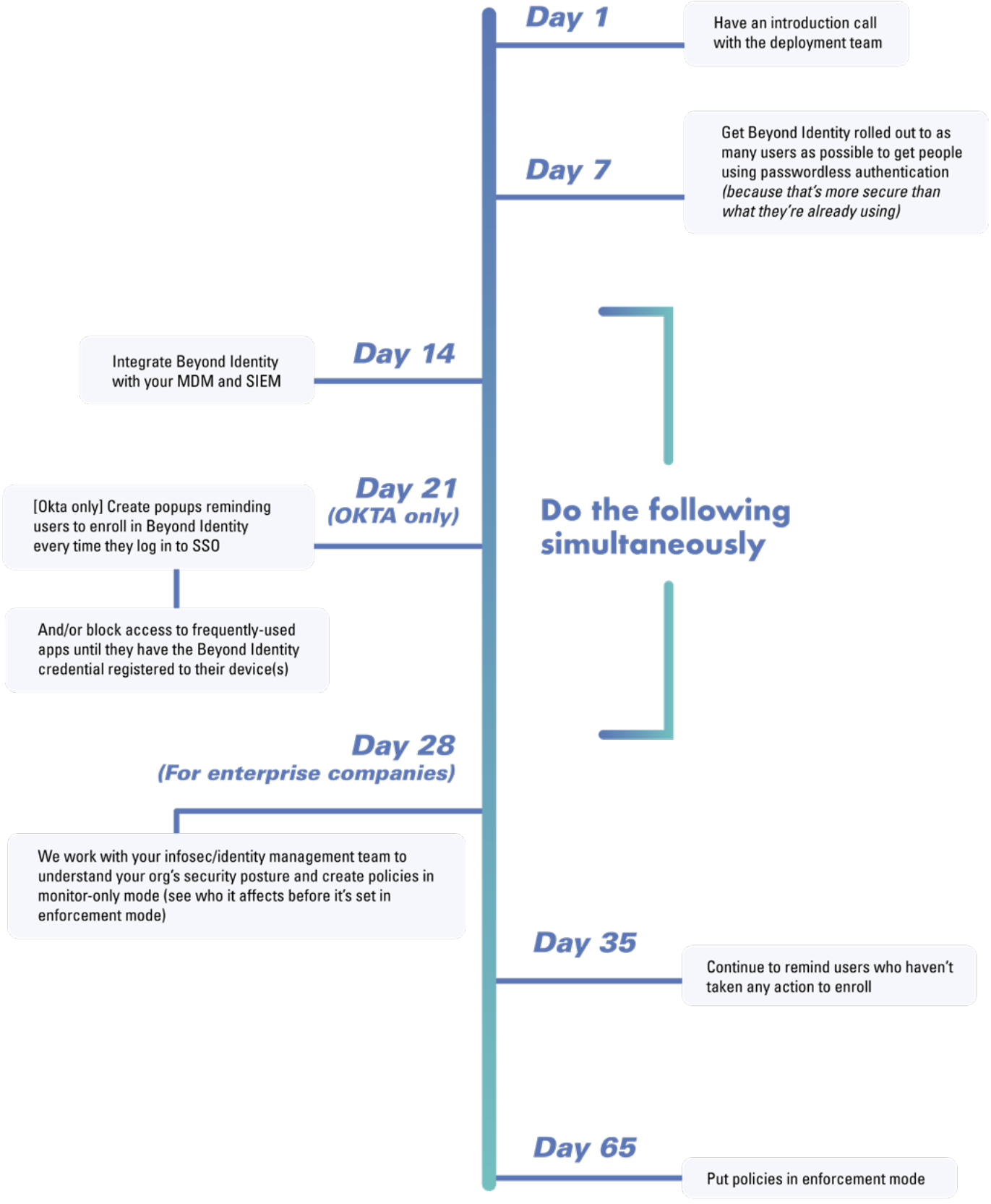
You will also meet your deployment engineer and a support team representative to ensure all your questions about deploying Beyond Identity and our comprehensive support as a customer are answered.

Q: Over time, how does my relationship with these points of contact change?

A: The deployment engineer will assist you in ensuring the required integrations and policies are in place, and everything is working as expected. Towards the end of the 90-day onboarding process, you will migrate the remainder of your users.

Your Customer Success Manager will become your primary contact upon deployment completion. Our goal is to ensure that your post-deployment runs smoothly and to direct any queries or requests to the appropriate party.

Of course, Customer Support will assist with technical inquiries (such as issues and feature requests) and help after onboarding ends. We aim to make your transition to passwordless as painless as possible and ensure that you're well supported from start to finish.


Day 1
Have an introduction call with the deployment team
Day 7
Get Beyond Identity rolled out to as many users as possible to get people using passwordless authentication (because that's more secure than what they're already using)
Day 14
Integrate Beyond Identity with your MDM and SIEM
Day 21 (OKTA only)
[Okta only] Create popups reminding users to enroll in Beyond Identity every time they log in to SSO
And/or block access to frequently-used apps until they have the Beyond Identity credential registered to their device(s)
Do the following simultaneously
Day 28 (For enterprise companies)
We work with your infosec/identity management team to understand your org's security posture and create policies in monitor-only mode (see who it affects before it's set in enforcement mode)
Day 35
Continue to remind users who haven't taken any action to enroll
Day 65
Put policies in enforcement mode