# XFA Onboarding Package


**1. Welcome & Orientation**

1.1. Welcome Message from XFA

Our Vision

Our Mission

Solution Overview

Our Promise

**2. Technical Onboarding**

2.1. Implementation Overview

2.2. Integration Guide

Phase 1: Device Discovery with XFA

Phase 2: Awareness

Phase 3: Policy Setup and Check Selection

Phase 4: Enforcing Device Health Checks

Phase 5: Monitoring and Feedback

2.3. Troubleshooting

**3. User Enablement**

3.1. Admin Communication Templates

Phase 1: Preparing the way for XFA

Phase 2: Rolling out XFA Awareness

Phase 3: Enforcing device health checks

3.2. FAQ for Employees

**4. Success Planning**

4.1. Success Metrics

Device Trends in Dashboard Statistics

Setting Goals

4.2. Example Reporting

**5. Internal Launch Kit**

# 1. Welcome & Orientation

## 1.1. Welcome Message from XFA

Welcome and thank you for choosing XFA as your trusted partner in securing your organization's devices and data. We're thrilled to have you on board.

This onboarding guide will walk you through every step of deploying XFA within your environment: from the initial setup to ongoing monitoring and optimization. Whether you manage a handful of endpoints or an enterprise-scale device fleet, this framework is designed to adapt to your organization's pace and needs.

At XFA, we believe that modern device security should empower, not restrict. Our commitment is to make device security seamless, scalable, and human-centered, so that securing your organization's data becomes frictionless and effective.

### Our Vision

*The only difference between devices used to work will be who paid for them — not how they are secured.*

This principle guides everything we build. We envision a world where security is not a burden, but an invisible layer of trust that follows every user and every device, wherever they work.

### Our Mission

*Secure anyone and everything accessing your company's data with pragmatic and privacy-centric solutions.*

Our mission is to help organizations protect their people, devices, and data through a solution that balances strong security with respect for privacy and flexibility. We believe in making device compliance clear, transparent, and frictionless, for both IT teams and employees.

## Solution Overview

XFA secures every device used for work by identifying risks and verifying compliance at login - while preserving privacy and requiring minimal effort.

XFA's platform completes and automates an organization's device security strategy — from full visibility and user awareness to scalable enforcement — all while reducing IT costs, eliminating overhead, and maximizing flexibility.

**Organizations work up through 3 stages:**

1. **XFA Discovery** allows security teams to gain full visibility into their organization's device security posture in just a few clicks — uncovering all unknown and ignored devices used for work, with no software or hardware installation required.

2. **XFA Awareness** automatically notifies users about security issues with any device they use for work — without requiring any software installation. It explains the organization's policy and provides a personalized, guided experience to resolve issues, helping users stay productive and avoid being denied access when out of policy.

3. **XFA Enforce** is the flagship feature that adds device security as an additional authentication factor — enabling users to start working from anywhere, on any device, as long as it meets security requirements. It provides early warnings, guides users through resolution, and ensures only safe devices are used for work.

## Our Promise

We promise to make your onboarding smooth, your rollout efficient, and your operations more secure from day one.

Here's what you can expect:

- A dedicated XFA implementation specialist to guide your setup.

- Clear documentation, practical examples, and tailored support.

- Real-time insights through the XFA Dashboard to measure progress and success.
- A commitment to continuous improvement; we evolve alongside your needs.

We're here to help you strengthen your security posture and give your teams the freedom to work securely!

Warm regards,
**Customer Success & Implementation Team of XFA**

---

**Support overview**

Support channels: dedicated Slack/Teams workspace (if applicable), email, or Intercom.

**Product updates**

- XFA Changelog
- Newsletter: optional subscription for new features and security updates.

# 2. Technical Onboarding

## 2.1. Implementation Overview

**Milestones Checklist:**

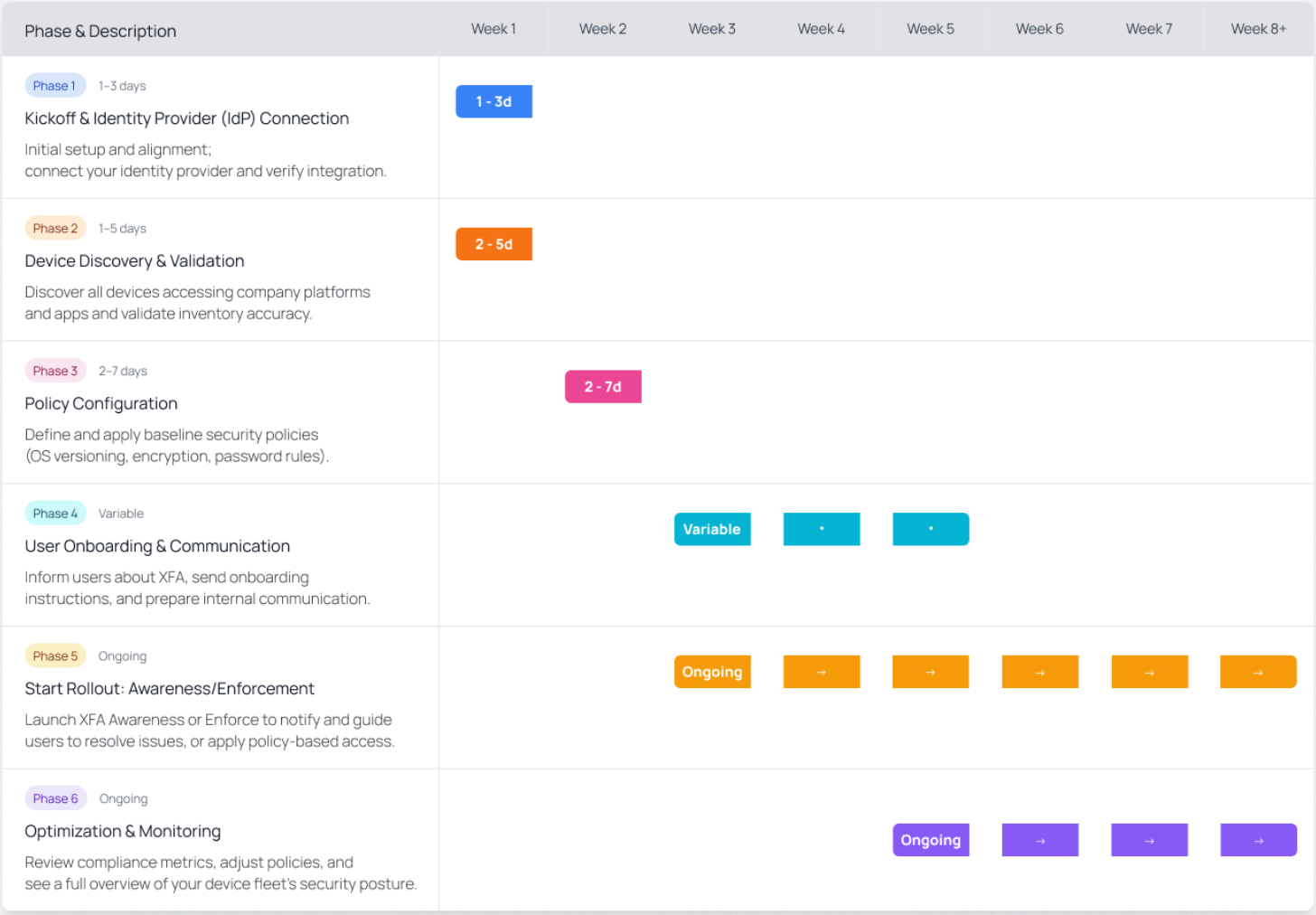
- ☐ Successful connection to the Identity Provider
- ☐ Device discovery
- ☐ Review of the device inventory
- ☐ Policy Setup
- ☐ Troubleshooting
- ☐ Monitoring

## 2.2. Integration Guide

This guide provides practical tips and recommendations for successfully implementing **XFA** in your organization. The goal is to minimize friction, ensure employees understand the benefits and usage, and reassure them about privacy protections.

### Project Timeline

Implementation phases and schedule overview



## Phase 1: Device Discovery with XFA

**Objective**: Seamlessly discover all devices within your organization without requiring employee intervention, by linking your identity provider.

1. **Set Up Device Discovery**
    - Begin the discovery process by connecting XFA to your organization's identity provider:
        - Okta
        - OneLogin
        - Google Workspace
        - Microsoft Entra ID

2. **Benefits of Discovery**
    - **No User Disruption**: Devices are identified without requiring manual input or action from end-users.
    - **Complete Visibility:** Gain an overview of all devices (corporate and personal) linked to your organization's identity provider.
    - **Simplified Setup**: Centralize device information before rolling out further compliance steps.

3. **Review Device Inventory**
    - Once discovery is complete, review the list of detected devices in the XFA Dashboard.
    - Verify that devices have been correctly identified and categorized (e.g., desktops, laptops, mobile devices).

By completing the Discovery Phase, your organization can achieve full device visibility, laying the foundation for compliance enforcement without creating unnecessary friction for employees.

---

## Phase 2: Awareness

**Objective**: Inform employees about their device compliance status and encourage them to take necessary actions to meet security policies.

1. **Configure Awareness Campaigns**
    - Navigate to the Awareness Tab in the XFA Dashboard.
    - Set up campaigns to notify specific groups of users based on their compliance status:
        - **Verification Email**: Sent to users whose devices have not been verified. This prompts them to install the XFA Mobile App to complete the verification process.
        - **Risk Email**: Sent to users whose devices do not meet the organization's defined security policies.
2. **Group Targeting**
    - Use group settings to target specific employees or departments for awareness emails.
    - For example, you want to rollout the awareness feature group per group within your organization
3. **Encourage User Action**
    - Employees receiving **verification emails** are guided through the process of installing the XFA App and verifying their devices.
    - Employees receiving **risk emails** are provided with detailed instructions on how to update their device to meet compliance requirements.

---

### Phase 3: Policy Setup and Check Selection

**Objective**: Define the compliance policies and device checks your organization requires for secure access.

1. **Access Policy Configuration**
    - Go to the Policies Tab in the XFA Dashboard.
    - Define the device checks that need to be enforced, such as:
        - Operating system version.
        - Screen lock or passcode enabled.
        - ...
2. **Custom Check Selection**
    - Choose from pre-configured checks or create custom policies tailored to your organization's security needs.

### Phase 4: Enforcing Device Health Checks

**Objective**: Enforce health checks to ensure devices meet compliance goal requirements before accessing work applications.

1. **Notify Employees of the Enforcement Date**
    - Communicate when compliance checks will become mandatory and emphasize the importance of addressing any device issues beforehand.
2. **Prepare for Increased Support Needs**
    - Anticipate an uptick in support requests and ensure IT resources are ready to handle inquiries.
3. **Monitor Compliance Progress**
    - Track compliance rates in the XFA Dashboard and reach out to users with unresolved issues.
4. **Reinforce Privacy Standards**
    - Remind employees that XFA only monitors essential security data and provides access to privacy settings for transparency.

---

### Phase 5: Monitoring and Feedback

**Objective**: Ensure long-term success by monitoring compliance and gathering feedback for continuous improvement.

1. **Monitor Compliance Metrics**
    - Regularly review compliance data to identify trends or recurring issues.
2. **Compliance Overview**
    - You can export reports to your GRC platforms such as Vanta, Drata, Trustcloud and Thoropass directly via integration.
3. **Collect Employee Feedback**
    - Use surveys or host feedback sessions to understand the user experience with XFA.
4. **Update Documentation**
    - Revise FAQs and guides based on insights gained during the rollout.
5. **Ongoing Support**

- Schedule periodic support sessions or provide updates on new features and security enhancements.

## 2.3. Troubleshooting

| Issue | Possible Cause | Resolution |
|---|---|---|
| Devices not syncing | Device is not yet affiliated. | After Phase 2 – Awareness<br>Ensure that after users install the application, they continue their flow in the browser. Installation alone is not sufficient, users must return to the browser that prompted the installation and complete the steps outlined there.<br><br>After Phase 4 – Enforcing Device Health Checks<br>Confirm that the XFA app remains running at all times after installation. Do not close it. Also verify that the app displays the message: "Sharing device status with 1 organization." |
| User cannot sign in via XFA after successful Microsoft authentication | Active sessions in Microsoft were not properly revoked after configuration changes. Old tokens or stale sessions prevented the new sign-in flow from completing successfully. | Revoke all existing sessions in Microsoft before reattempting login. |

| | | |
|---|---|---|
| User unable to log in after email domain change | The user's UPN (User Principal Name) was updated in Microsoft Entra ID, but cached sessions or linked identities in XFA still referenced the old domain. As a result, authentication failed and the account became blocked. | Revoke old sessions and ensure the new UPN is synchronized correctly. |

# 3. User Enablement

## 3.1. Admin Communication Templates

Utilize the following email and message templates to prepare your team for the rollout of XFA. Before sending, make sure to customize the highlighted sections based on your specific situation.

### Phase 1: Preparing the way for XFA

| **Email: Introduction to XFA** | |
|---|---|
| **Recommended use:** Send via email 14 to 30 days before rolling out XFA | **Subject:** [IMPORTANT] Introducing XFA for a Safer Workplace |

Hi Team,

We are excited to share an important update about our security approach. Starting on [deploy date], we will begin introducing XFA to help keep our digital workspace secure. This message contains an overview of this tool and how it will impact you.

**What is XFA?**

XFA is a security tool that ensures all devices meet important security standards before they can access work apps. For example, if software is up to date and that disk encryption is enabled. In the future, when you sign into an app protected by [Insert IdP], XFA will run checks to confirm your device is healthy. If anything needs your attention, you will be provided with step-by-step instructions on what to fix before you finish logging in.

**How does XFA protect your privacy?**

XFA only collects essential data to confirm that your device meets security requirements for accessing work applications. It does not track your location, personal files, or browsing history. **Check this easy and simple walkthrough to experience how a device check with XFA happens:** Device Verification Walkthrough

**What is the rollout timeline?**

We will be rolling out XFA over the coming weeks. Here are some key dates:

- **[Deploy date]** – XFA will be rolled out to all devices. You'll see the menu bar app appear and will notice checks running when you sign in to apps.
- **[Check enforcement date]** – We'll start enforcing device health checks. If your device fails any checks, you'll need to resolve the issue before signing in.

We understand that adapting to new tools can be a shift, and we're here to make this process as smooth as possible. By taking this step, we are enhancing our security posture while minimizing the impact on your day-to-day work.

You can learn more about XFA on this page. If you have any questions or concerns, don't hesitate to reach out: [email] or [channel].

Thank you,
Your IT Team

## Slack/Teams Message: Introduction to XFA

**Recommended use:** Send via messaging platform 1 week before XFA rollout

**Exciting Security Update: XFA Rollout! 🚀**

Hey Team! Starting on [effective date], we're rolling out XFA to strengthen our digital security. Here's a quick overview:

🔍 **What is XFA?**
XFA ensures all devices meet our security standards before accessing work apps. Each time you log in, it checks for key items like software updates and malware protection. If anything needs attention, XFA will guide you on how to fix it before completing your sign-in.

🔒 **Privacy First**
XFA respects your privacy by only collecting essential security data. It doesn't track your location, personal files, or browsing history.

🔔 **How Will You See It?**

- **During sign-in:** XFA will check your device's compliance as you log in.
- **Menu Bar App:** You'll get helpful updates on any security issues needing attention.

🗓️ **Rollout Timeline:**

- **[Deploy date]:** Awareness mails are being sent
- **[Check enforcement date]:** Compliance checks will begin to be enforced

We appreciate your support as we make our workspace safer for everyone. Learn more about XFA on this page, or if you have questions, feel free to reach out via [email] or [channel]!

Thanks!

## Phase 2: Rolling out XFA Awareness

| **Email: XFA Rollout** | |
|---|---|
| **Recommended use:** Send email when you begin deploying XFA Awareness | **Subject:** [Action Needed] We're Now Rolling out XFA |

Hi Team,

We're pleased to announce that we are beginning to roll out XFA to strengthen device security across our organization. You'll need to install the XFA on your device next time you log in to an app protected by [our IdP].

**What You Need to Do**
The first time you sign into a protected app, you'll be prompted to install XFA. Follow the prompts to complete installation and register your device. To ensure a smooth setup, please complete the XFA installation on your primary work device first.

Once installation is complete, you'll see the XFA icon appear in your menu bar, providing quick access to your device's security status.

**What's Next?**
After you've installed the agent, you may begin seeing health checks running as you log in, checking for essential security items. At this stage, you will not be asked to fix any issues that are identified. Visit this page to learn what is happening on your device.

We plan to begin enforcing device health starting on [enforcement date], after which you'll need to follow step-by-step instructions to address any security problems before signing in to certain work apps. We'll send reminders and additional guidance as we approach this date.

**Support and Questions**

You can learn more about XFA here. If you have questions or encounter any issues with installation or setup, please reach out to our team via [email] or [channel]. We're here to support you throughout this process.

Best regards,
Your IT Team

## Slack/Teams Message: XFA Awareness Rollout

**Recommended use:** Send via messaging platform when you begin deploying XFA Awareness

**🚀 XFA Rollout Begins!**

Hi Team! We're rolling out **XFA** to strengthen our device security. You may be prompted to install XFA the next time you log into an app protected by [our IdP] if you're using a device that did not automatically install the tool.

**What to Expect:**

1. **Install & Register**: In the following weeks, you'll receive a verification mail. Tap the verification button, follow the prompts to install XFA on your device.
2. **XFA Icon**: After setup, you'll see the XFA icon in your menu bar for quick access to device health info.

**What's Next?** For now, health checks are informational only. Starting [enforcement date], you'll need to resolve any flagged issues before logging in. We'll share reminders as that date approaches!

**Privacy Reminder**: XFA only collects essential security data and does not track personal files, browsing history, or location.

**Need Help?**
Our team is here for any questions or setup support – just reach out via [email] or [channel]. You can also learn more about XFA here.

**Thanks,**
**IT Team**

### Phase 3: Enforcing device health checks

| **Email: Enforcing Device Health** | |
|---|---|
| **Recommended use:** Send via email the day you begin enforcing device health before login | **Subject:** Update: You'll Need to Resolve Security Issues Before Logging In |

Hi Team,

Starting today, if XFA detects a security issue during login, you'll need to resolve the problem before accessing certain work apps. Step-by-step instructions will be provided so that you can quickly make needed changes and continue on your way.

Privacy Reminder: XFA only collects essential security data and does not track personal files, browsing history, or location.

If you need assistance or have questions, please reach out to our support team via [email] or [channel] – we're here to help!

Thank you,
Your IT Team

**Slack/Teams Message: Enforcing Device Health**

**Recommended use:** Send via messaging platform when you begin enforcing checks

🔒 **XFA Health Checks Now in Effect**

Hi Team! Starting today, if **XFA** finds a security issue during login, you'll need to resolve it before accessing certain work apps. Don't worry—step-by-step instructions will guide you through the process to quickly get you back on track.

You can learn more about XFA here. As always, reach out to our support team with any questions via [email] or [channel] —we're here to help!

**Thanks,**
**IT Team**

## 3.2. FAQ for Employees

Frequently Asked Questions About XFA:

**Q: How does this tool impact my privacy?**
A: XFA respects your privacy by only collecting essential security data needed to confirm your device meets company standards. It does not track your personal files, browsing history, or location.

---

**Q: Do I have to install this on personal devices?**
A: XFA needs to be installed on any device you use to access work apps. However, if you do not use a personal device for work, you don't need to install it there. If you do use a personal device, rest assured that the tool focuses only on essential security checks and respects your privacy.

**Q: How can I register additional devices after adding my primary work device?**
A: When you log into a protected app on a new device, you will be prompted to install and register XFA on that device. Follow the same steps as with your primary work device to complete registration. Just please make sure you register your primary work device first as that is used to validate additional registrations in your name.

**Q: What happens if my device fails a health check?**
A: If XFA identifies an issue, you'll receive step-by-step instructions on how to resolve it. Most fixes are simple, like updating software or enabling malware protection. Once the issue is resolved, you'll be able to access work apps again.

**Q: Will XFA block me from logging in without warning?**
A: In most cases, no. XFA will typically notify you in advance if there are issues with your device that need attention. You'll also have a grace period to resolve the issue before it impacts your ability to log in.

**Q: What should I do if I can't resolve an issue on my device?**
A: If you run into trouble, reach out to IT support for assistance. Our team is here to help you troubleshoot and get your device back into compliance as quickly as possible.

**Q: Does XFA slow down my computer?**
A: No. XFA runs lightweight checks during login and occasionally in the background. It is designed to have minimal impact on your device's performance.

**Q: Can I use the skip option to log in without fixing an issue?**
A: In certain cases, you may be able to skip blocking for a short period. However, this may not

be available for critical security issues. Check with IT if you have specific questions about this feature.

---

**Q: Do I need to keep the XFA menu bar app open?**
A: Yes, the XFA menu bar app is a key part of XFA. It notifies you of any issues with your device and provides quick access to instructions for resolving them.

---

**Q: How often will XFA run checks?**
A: XFA runs a brief check each time you log in to a protected app and occasionally in the background to monitor compliance. You'll only be notified if there's an issue needing your attention.

---

**Q: Will I get in trouble if my device fails a health check?**
A: No, failing a health check simply means there's a security issue that needs to be addressed. XFA provides guidance to help you resolve it, and IT is here to support you if needed.

# 4. Success Planning

## 4.1. Success Metrics

### Device Trends in Dashboard Statistics

The device trends feature provides valuable insights into your organization's security posture by displaying historical data and patterns. You can visualize how your device fleet's compliance has evolved, making it easier to identify security trends and take proactive measures.

You can view trends for:

- OS Out of Date: how many devices have outdated operating systems over time
- Device encryption compliance
- Browser security status
- Screen lock trends

## 4.2. Example Reporting

With XFA, it's easy to access and share your organization's device security insights and success metrics. You can export a full PDF of your device security overview directly from the dashboard, providing a clear snapshot of your environment's health and compliance status.

Each report includes a summary of security checks, key health insights, and a list of common vulnerabilities, which gives you a complete view of your device security posture.

It's perfect for internal reviews, compliance reporting, or executive updates, helping your team communicate progress and maintain visibility without manual effort.

See an example of such a report here: Device Security Report Example

# 5. Internal Launch Kit

**Logos:**

- PNG
- SVG
- White & dark background variants

You can find the logo files here.

**Announcement Email** (see templates above)

**Slack/Teams Message** (see templates above)