DocMagic MFA Customer Guide

Multi–Factor Authentication (MFA)

- DocMagic is enhancing account security by introducing **Multi–Factor Authentication (MFA).**

- MFA adds an extra layer of protection to your account by requiring a verification code from an authenticator application in addition to your username and password.

- **This Guide Explains:**
  - 🔐 MFA Overview & Benefits
  - 👥 Eligible Users & Shared Accounts
  - 📱 Supported Authenticator Apps
  - 🚀 First–Time MFA Setup
  - 🔑 Future Logins
  - 🔒 Password Resets & Account Recovery
  - 🔗 External System Access
  - 📲 Device Changes & MFA Resets
  - ❓ Frequently Asked Questions (FAQs)

What is MFA?

- Multi-Factor Authentication (MFA) is a security feature that helps verify your identity when signing in.
- Instead of relying only on a password, MFA requires a second verification factor, such as a temporary code generated by an authenticator application.

Without MFA

👤 Username
🔑 Password

With MFA

👤 Username
🔑 Password
📱 Verification Code from an Authenticator App

- Even if someone obtains your password, they will still need access to your authenticator app to gain access to your account.

Why is DocMagic Introducing MFA?

MFA helps:

- Protect customer accounts
- Reduce risks from stolen or compromised passwords
- Improve security for sensitive business processes
- Align with modern security standards used across the financial services industry
- Provide secure authentication without requiring text messages or phone numbers

Who Will Use MFA?

Included in Phase 1

- MFA applies to customer users who log in directly through the DocMagic website when MFA has been enabled for their account.

Not Included in Phase 1

- The following users are not included in the initial release:
  - Borrowers
  - Notaries
  - Settlement Agents
  - Other identity-based users
  - Federated Single Sign-On (SSO) users

💡 Organizations using SSO are expected to manage MFA through their own identity provider

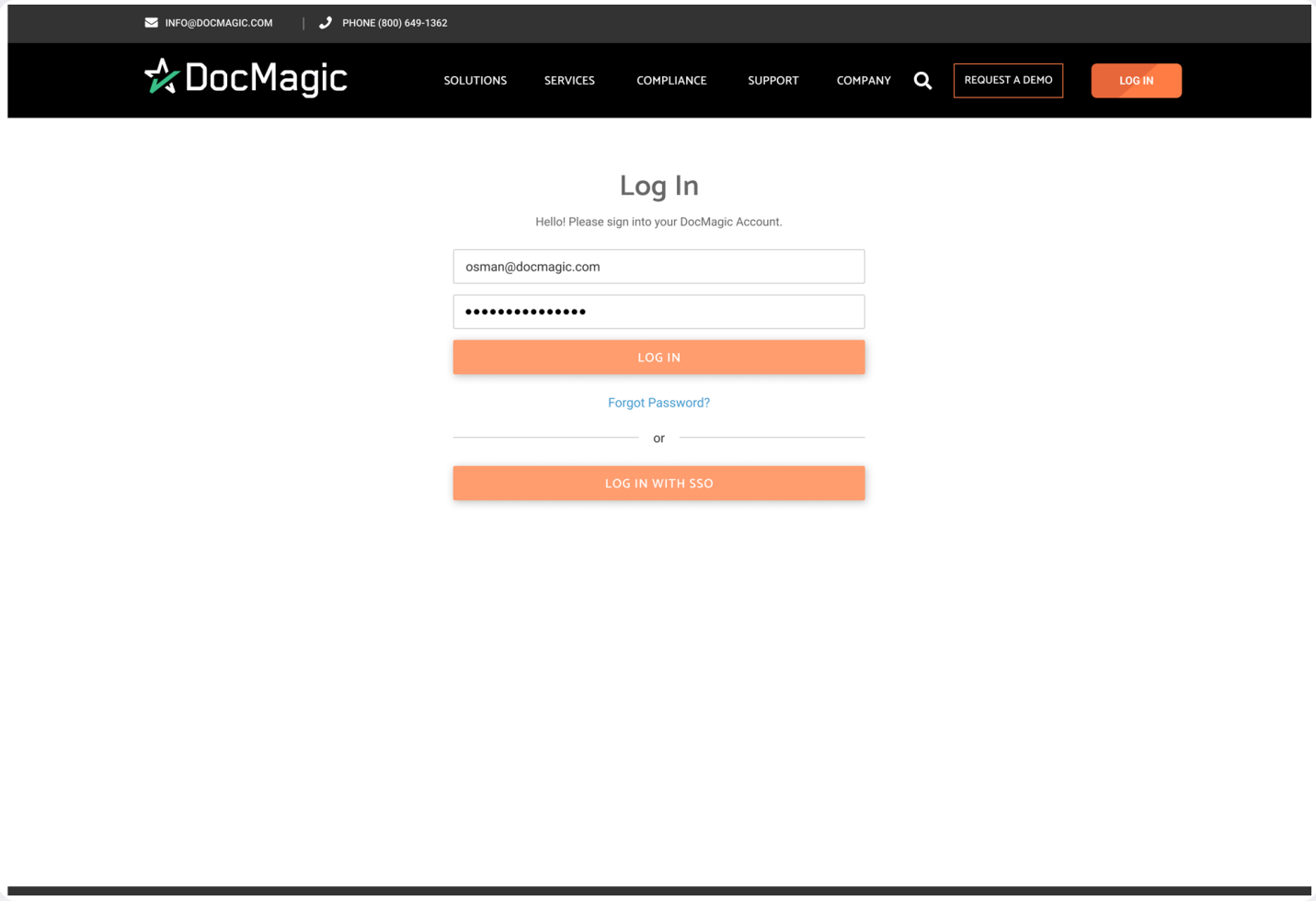
Before You Get Started

- Have your username and password ready
- Download a supported authenticator app:
  - Microsoft Authenticator
  - Google Authenticator
  - Duo Mobile
  - Other compatible authenticator apps
- Have your mobile device available during setup

Supported Authenticator Apps

- DocMagic supports standard authenticator applications that generate time-based verification codes.
- **Examples include:**
  - Microsoft Authenticator
  - Google Authenticator
  - Duo Mobile
  - Other compatible authenticator applications
- You may use the authenticator app that best fits your organization's requirements.

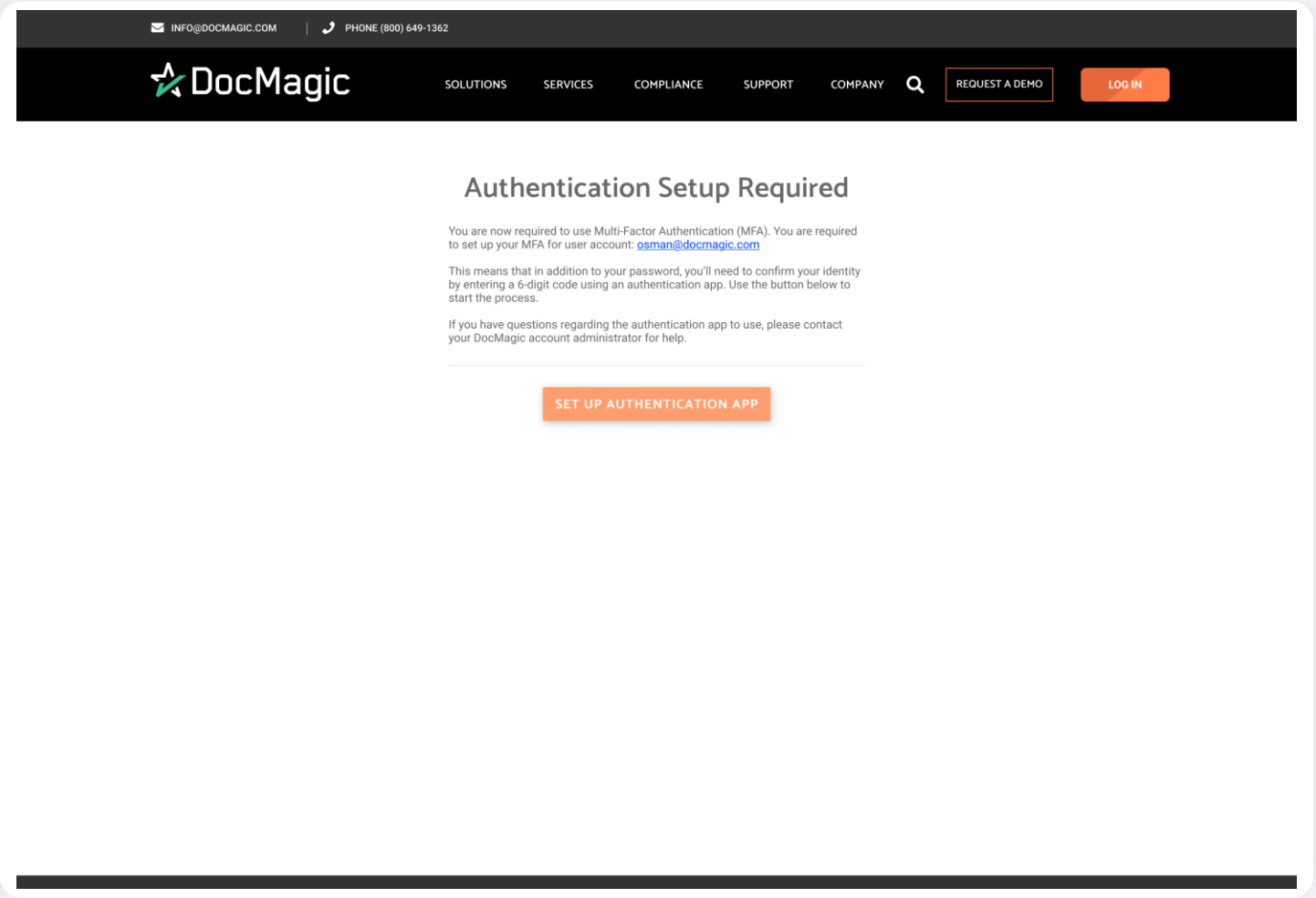
First–Time MFA Setup



1. Sign In

- Go to the DocMagic login page
- Enter your Username and Password
- Click Log In

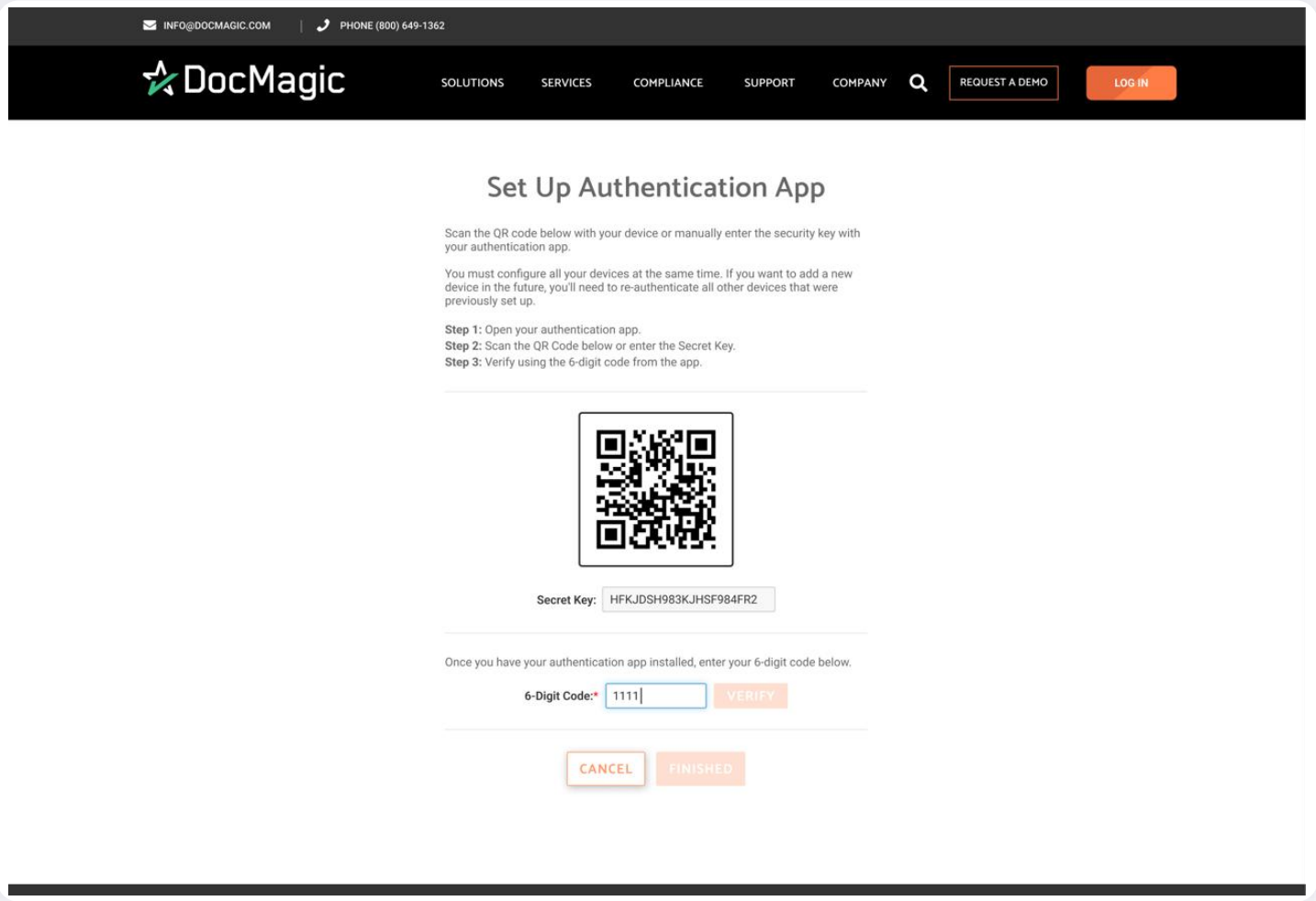
First–Time MFA Setup



2. Set Up Your Authenticator App

- When prompted click: **Set Up Authentication App**

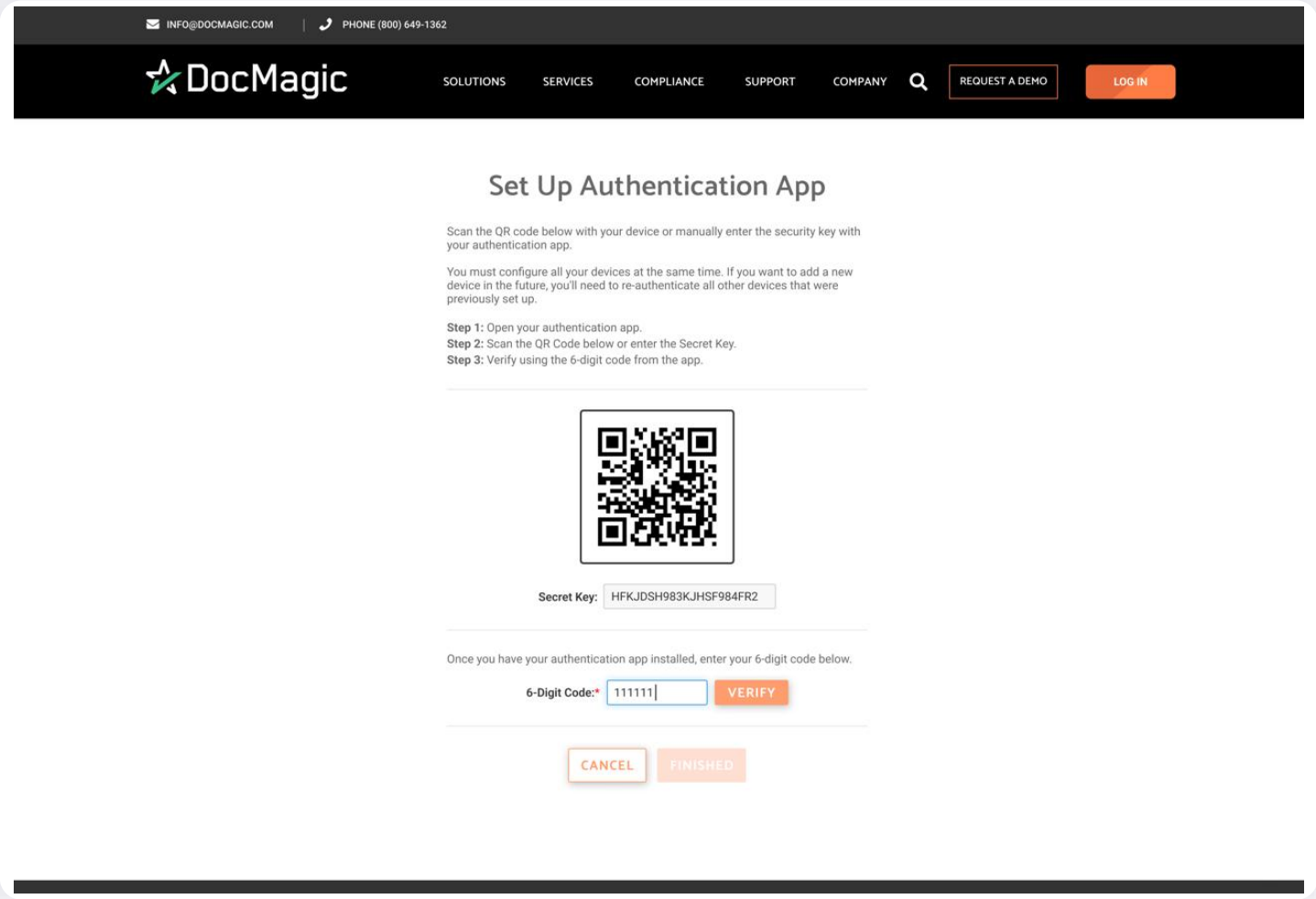
First–Time MFA Setup



2. Set Up Your Authenticator App

- You'll receive:
  - QR Code
  - Secret Key
  - Verification field
- Open your authenticator app and:
  - Scan the QR Code or
  - Enter the Secret Key manually
- Your app will begin generating 6–digit verification codes.

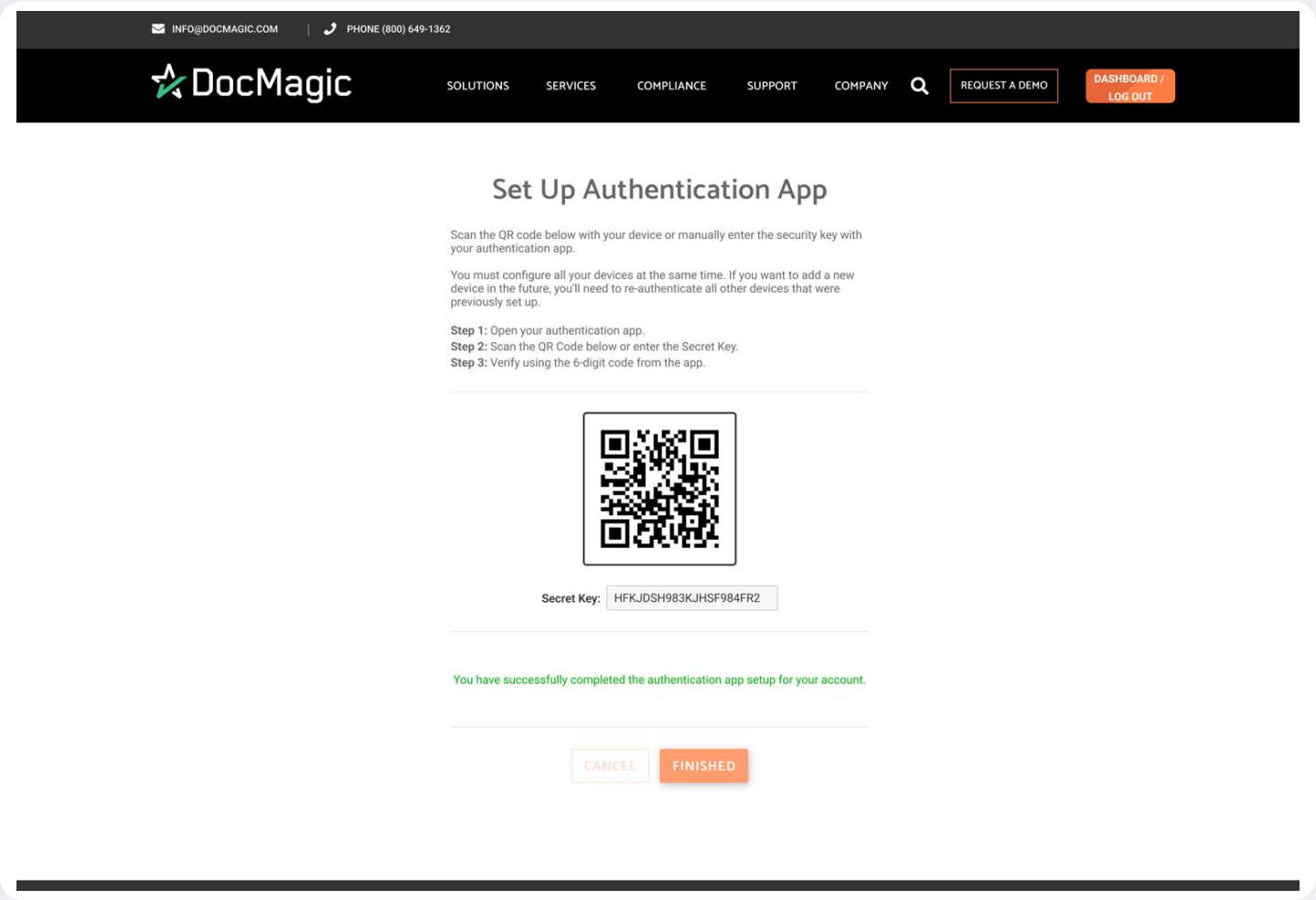
First–Time MFA Setup



3. Verify Enrollment

- Enter the current 6–digit code
- Click Verify

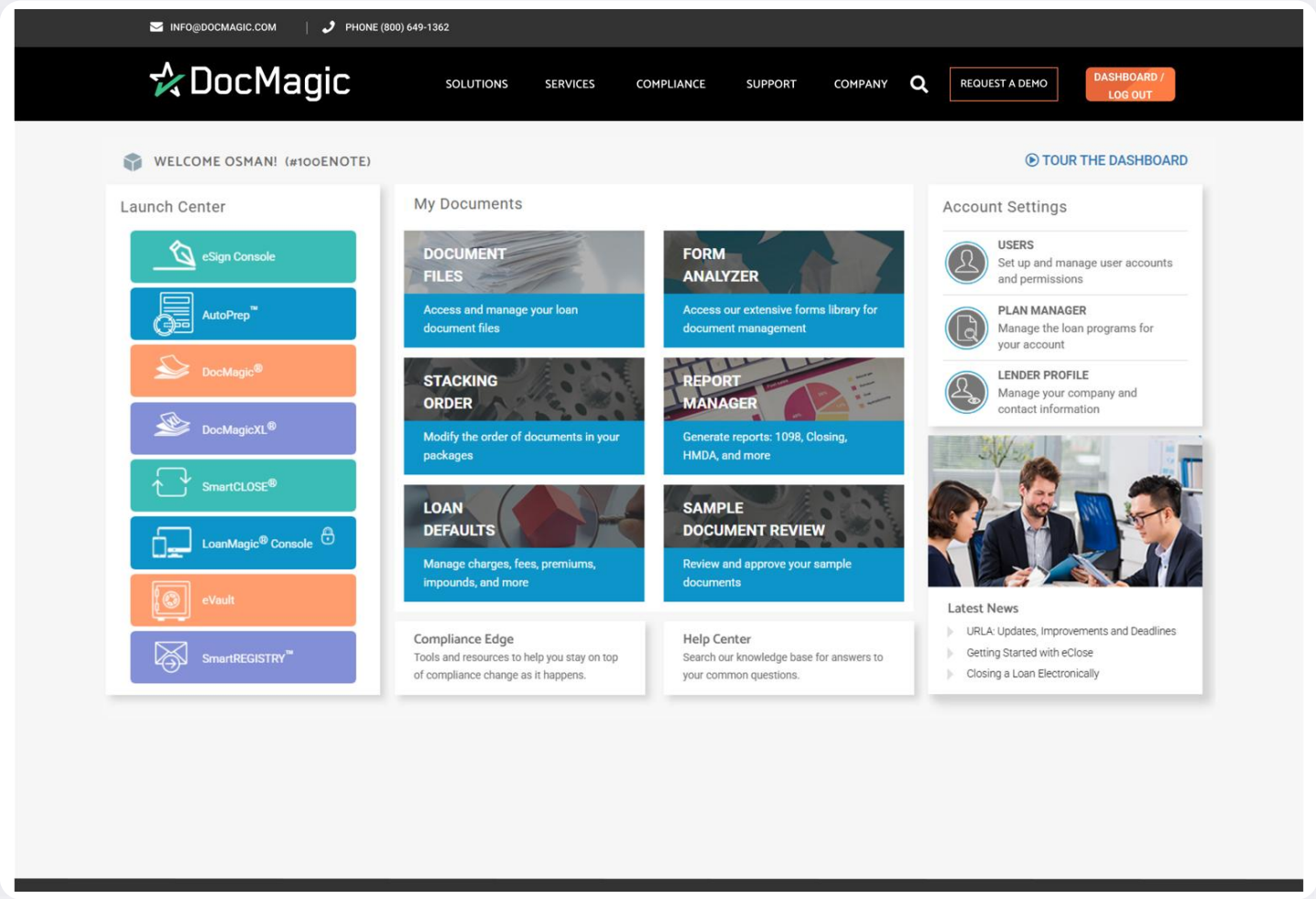
First–Time MFA Setup



3. Verify Enrollment

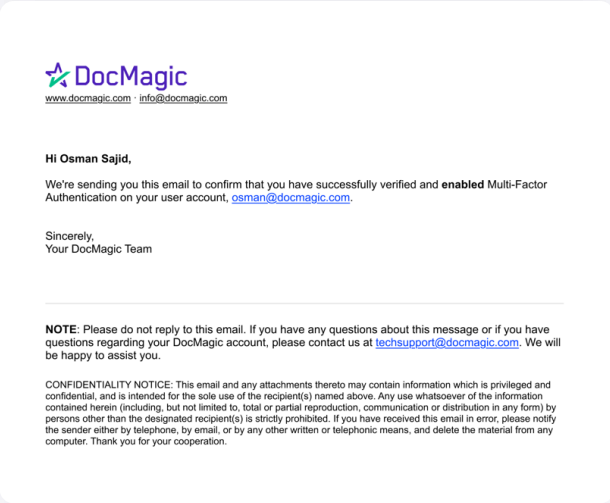
- Setup Message:
  - *You have successfully completed the authentication app setup for your account.*
- Finished button becomes enabled & selected.
- **Important:** Register all devices (work phone, personal phone, tablet) during initial setup.

First–Time MFA Setup



3. Verify Enrollment

- Setup Complete
- You will be directed to your Dashboard.
- MFA enrollment is completed.
- Confirmation email is sent.



DocMagic
www.docmagic.com · info@docmagic.com

Hi Osman Sajid,

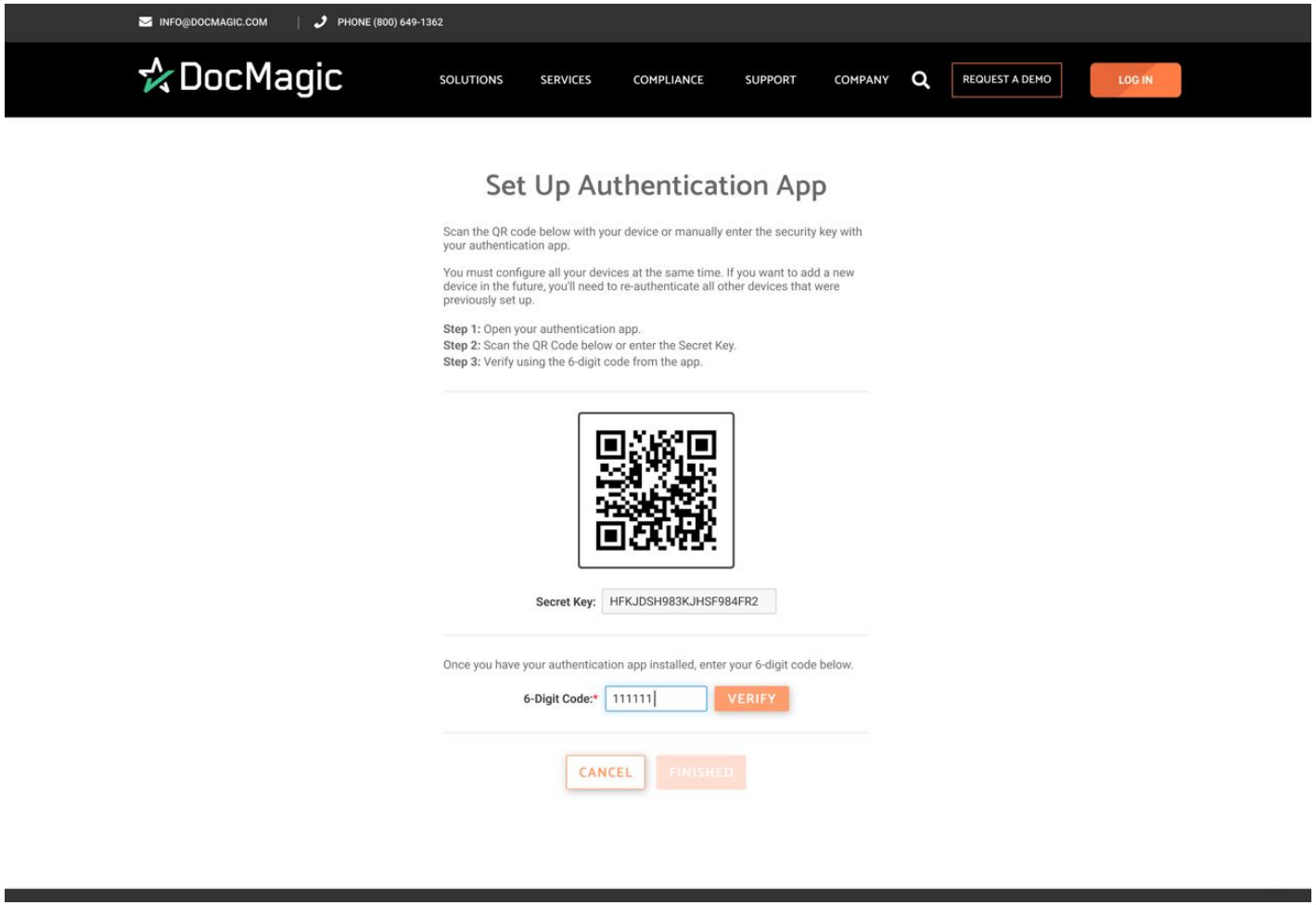
We're sending you this email to confirm that you have successfully verified and **enabled** Multi-Factor Authentication on your user account, osman@docmagic.com.

Sincerely,
Your DocMagic Team

NOTE: Please do not reply to this email. If you have any questions about this message or if you have questions regarding your DocMagic account, please contact us at techsupport@docmagic.com. We will be happy to assist you.

CONFIDENTIALITY NOTICE: This email and any attachments thereto may contain information which is privileged and confidential, and is intended for the sole use of the recipient(s) named above. Any use whatsoever of the information contained herein (including, but not limited to, total or partial reproduction, communication or distribution in any form) by persons other than the designated recipient(s) is strictly prohibited. If you have received this email in error, please notify the sender either by telephone, by email, or by any other written or telephonic means, and delete the material from any computer. Thank you for your cooperation.

Future Logins



- After completing enrollment, future logins are simple.

    1. Enter Username & Password
    2. Open Authenticator App
    3. Enter Current 6–Digit Code
    4. Click Verify
    5. Access Dashboard

- MFA only needs to be enrolled once.

Multiple Accounts?

- One MFA registration works across all DocMagic accounts.

New Phone or Lost Device

If you lose access to your authenticator app:

1. Contact your Account Administrator
2. Request an MFA Reset
3. Log in again
4. Complete MFA enrollment on the new device

⚠ Previous QR codes and verification codes will no longer work after a reset.

NEED HELP?

- **Contact Your Administrator**
  - New phone
  - Lost device
  - Locked account
  - MFA reset assistance

Contact DocMagic Support

- QR code does not display
- Setup cannot be completed
- Valid codes are repeatedly rejected
- Unable to access Dashboard after verification

Troubleshooting

Verification Code Not Working?

- Use the newest displayed code
- Verify you're using the correct authenticator app
- Wait for a new code and try again
- Ensure your device date/time updates automatically

Account Locked?

- Five consecutive invalid MFA codes will lock the account.
- Contact your Administrator for assistance.

💡 Quick Tip

- To avoid future access issues, enroll all devices you plan to use during your initial MFA setup, including work phones, personal phones, and tablets.

Shared User IDs and Service Accounts

Some organizations use shared user IDs or service accounts for business processes such as:

- Document generation
- Integrations
- API-related activities

- These accounts often use a generic email address
- For example: *lendername@lender.com* rather than an email address assigned to a specific individual.

Shared User IDs and Service Accounts

Important Considerations for MFA

- Multi-Factor Authentication (MFA) is designed for accounts that are associated with a single user.
- Organizations that use shared user IDs should review how MFA will be managed within their organization before MFA is enabled.

When a Shared Account Is Configured for MFA:

- The authenticator application must be accessible to individuals authorized to use that account.
- Organizations are responsible for determining how access to the authenticator application will be managed.
- Users may need access to the account's authenticator application whenever they log in directly through the DocMagic website

Shared User IDs and Service Accounts

Password Reset and Account Unlocks

- Service accounts and shared user IDs may occasionally require password resets or account unlocks.

If a Password Reset or Account Unlock is Required:

- Sign in to the DocMagic website using the shared account.
- Complete the password reset or account recovery process.
- Continue with MFRA authentication if prompted.

Access Through External Systems

Many shared user IDs are primarily used through:

- Loan Origination Systems (LOS)
- Direct API Integrations
- Other integrated third-party platforms

- These integrations are **not impacted by DocMagic MFA** when authentication is managed by the external system.
- However, users who access the same account directly through the DocMagic website may be required to complete MFA, depending on their organization's configuration.

Shared User IDs and Service Accounts

Recommendation

- If your organization uses shared user IDs or service accounts, review your internal procedures before MFA is enabled to ensure authorized users can:
    - Continue to access the account
    - Complete password resets
    - Perform account recovery activities
    - Avoid interruptions to business processes

Frequently Asked Questions

Do I need MFA every time I log in?
Yes. If MFA is enabled for your account, you'll be required to enter a verification code each time you create a new login session.

Will I receive verification codes by text message or email?
No. DocMagic MFA uses an authenticator application and does not send verification codes through SMS or email.

Which authenticator app should I use?
You may use any compatible authenticator app that supports time-based verification codes, including:
Microsoft Authenticator
Google Authenticator
Duo Mobile
Your organization may choose the app that best meets its requirements

Can I skip MFA setup?
No. When MFA is enabled for your account, enrollment must be completed before access to DocMagic is granted.

Can I add another phone or device later?
Additional devices should be enrolled during your initial MFA setup. If you need to add or replace a device later, contact your administrator for assistance.

Will I be signed out immediately if MFA is enabled while I'm already logged in?
No. Your current session will remain active. MFA will be required the next time you sign in.

What happens if I forget my phone?
You will need assistance from your administrator to reset your MFA enrollment before you can access your account again.

Frequently Asked Questions

Does MFA apply when accessing DocMagic through an LOS, POS, or other integrated platform?

No. MFA only applies when users log in directly through the DocMagic website. Authentication for integrated platforms is managed independently by those systems.

How does MFA work for shared user IDs or service accounts?

MFA is intended for accounts associated with a single individual. Organizations that use shared user IDs or service accounts should determine how they will manage access to the authenticator application used by that account. Users accessing the account directly through the DocMagic website may be required to complete MFA authentication, while access through LOS platforms or API integrations is generally managed by those external systems.