

SecureID – Usage Guide

A lightweight identity-verification tool for IT Helpdesks

Overview

SecureID is a lightweight web application designed to help IT support teams securely verify user identities and perform privileged actions such as password resets and MFA clearing.

Users can be validated through either:

- **Phone Verification** (voice call with verification code)
- **Digital ID Verification** (Microsoft Entra Verified ID / Authenticator-based credential)

Images displayed in this guide reflect the UI shown in the uploaded document pages.

1. Accessing the Application

Navigate to the SecureID web portal:

`https://secureid-xxxxxxxxxxxxxxxx.azurewebsites.net`

A custom domain (e.g., `x@company.com`) may be added later.
(URL anonymized)

2. Sign In

Authenticate using your organization's SSO / Microsoft 365 account.
If you are already logged in, the app will automatically forward you.

3. Start a Verification

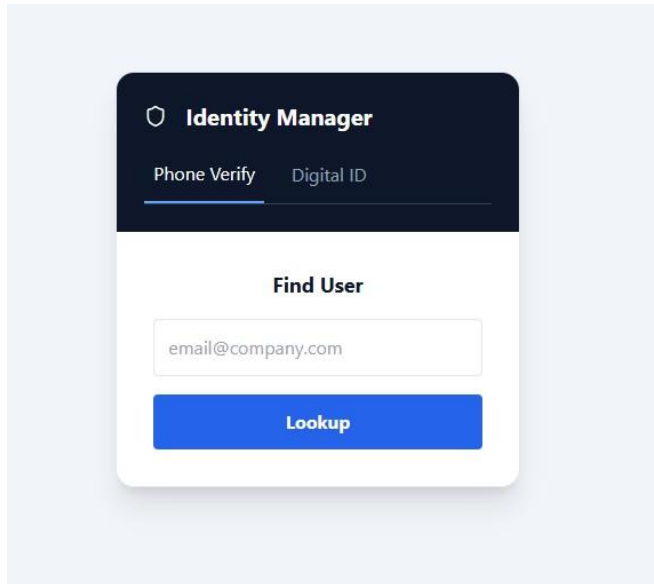
You may choose between:

Phone Verification

Send a verification call to the phone number on record for the user.

Digital ID Verification (Preview)

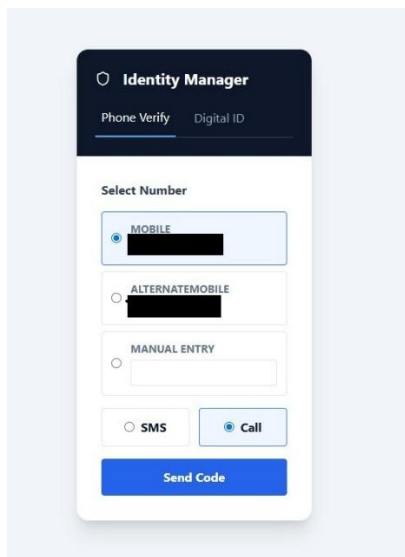
Allows identity validation through Microsoft's Verified ID framework using a QR code scanned via Microsoft Authenticator.



4. Retrieve Authentication Methods

When searching by email, SecureID queries the directory and returns all phone-based authentication methods available for that user.

Extensions should work, though edge-case behavior is still being validated.



5. Phone Call Verification

1. The user receives an automated call.
2. The spoken verification code **must match** the code displayed on your screen.
3. Once validated, SecureID confirms successful identity verification.

After verification, you may:

- **Reset the user's password** (14+ characters)
- **Revoke active sessions**
- **Reset MFA methods** (*Microsoft has begun restricting some automated resets*)

The screenshot shows the 'Identity Manager' application interface. At the top, there's a dark blue header with a shield icon and the text 'Identity Manager'. Below the header, there are two tabs: 'Phone Verify' (selected) and 'Digital ID'. The main content area is white and contains a yellow box with the text 'Code sent! Ask user to read it back.' Below this is a light blue box with the text 'Admin Note: Code is 603410'. A white input field displays the code '603411'. Below the input field is a blue button labeled 'Verify'. At the bottom, there is a pink box with the text 'Incorrect code'.

The screenshot shows the 'Identity Manager' application interface after successful verification. The header and tabs are the same. The main content area is white and contains a green box with the text 'Success!' and 'Phone Verified.' Below this are three buttons: a blue button labeled 'Reset Password (14+ Chars)', a purple button labeled 'Revoke Sessions & Reset MFA', and a dark blue button labeled 'Start Over'.

6. Digital ID Verification (Optional)

Digital ID verification requires:

- A **Verified Credential** (e.g., "VerifiedEmployee") created under Microsoft Entra Verified ID.
- Your SecureID App Service URL added to Verified ID **Trusted Domains**.

When initiated, the tool displays:

- A **QR code** for the user to scan.
- Buttons to **email the link**, copy the QR, or copy the deep link.

Once verified, the UI confirms identity and enables password and MFA management actions, just like phone verification.

