

Multi-Factor Authentication (MFA) in ServiceNow: Implementation Guide

Contents

1. Introduction	3
2. Benefits of MFA	3
3. Prerequisites	3
4. MFA Methods Supported in ServiceNow	3
5. Implementation Steps.....	4
A. Enabling MFA in ServiceNow	4
B. Testing the Implementation	8
6. Best Practices	8
Multi-Factor Authentication (MFA) in ServiceNow: Implementation Guide.....	9
Table of Contents	9
1. Introduction	9
2. Benefits of MFA.....	9
3. Prerequisites	9
4. MFA Methods Supported in ServiceNow.....	9
5. Implementation Steps.....	10
A. Enabling MFA in ServiceNow	10
B. Configuring Identity Providers	10
C. Setting Up MFA for Users	10
D. Testing the Implementation.....	10
6. Best Practices	11
7. Troubleshooting	11
8. Conclusion.....	11

1. Introduction

Multi-Factor Authentication (MFA) enhances the security of user logins by requiring multiple forms of verification. Implementing MFA in ServiceNow ensures that only authorized users can access the system, thereby safeguarding sensitive data and applications from unauthorized access.

2. Benefits of MFA

- **Enhanced Security:** Reduces the risk of compromised credentials.
- **Compliance:** Helps meet regulatory requirements.
- **User Confidence:** Boosts trust by protecting user data.
- **Risk Mitigation:** Decreases the likelihood of security breaches.

3. Prerequisites

Before implementing MFA in ServiceNow, ensure the following:

- An active ServiceNow instance with admin access.
- A compatible identity provider (IdP) that supports MFA.
- Users' devices configured for receiving MFA tokens (e.g., mobile phones for SMS, authentication apps).

4. MFA Methods Supported in ServiceNow

ServiceNow supports various MFA methods, including:

- **SMS-Based OTP:** One-time password sent via SMS.
- **Email-Based OTP:** One-time password sent via email.
- **TOTP Apps:** Time-based One-Time Password applications like Google Authenticator or Authy.
- **Push Notifications:** Using apps like Duo Mobile for approval requests.

5. Implementation Steps

A. Enabling MFA in ServiceNow

1. Enable required plugin:

- Enable “Integration Multifactor Authentication” Plugin from Application manager

The screenshot shows the ServiceNow Application Manager interface. At the top, there's a navigation bar with links for 'Activity log', 'Switch to Classic App Manager', 'Request plugin', and 'Open store'. Below the header, a large banner for the 'Integration - Multifactor Authentication' plugin is displayed. The banner includes a green circular icon with a puzzle piece, the plugin name, its Now Platform Security status, and its plugin ID. A 'Summary' section on the left contains a brief description of the plugin's purpose. In the center, a 'Get started' box displays a message indicating the application is installed and ready for use. On the right, a 'Quick Actions' section has a 'Repair' link. The overall theme is dark with blue and white text.

2. Navigate to the Multi-Factor Authentication Settings:

- Go to Multi-Factor Authentication > Settings in the ServiceNow instance.
- Toggle the MFA option to enable it for your instance.
- Choose the desired MFA methods (SMS, Email, TOTP, Push Notifications).

The screenshot shows the 'Multi-factor Authentication Properties' configuration page. On the left, a sidebar menu is open under 'Properties', specifically 'Web Authentication'. The main area contains several configuration fields:

- 'Enable Multi-factor authentication' checkbox: checked.
- 'Number of times a user can bypass setting up multi-factor authentication': input field set to 3.
- 'The time in minutes, the one time code sent to user's email address is valid for': input field set to 5.
- 'Additional time in seconds for which the code will be valid to accommodate for the clock skew. Max value is 60 seconds.'': input field set to 10.
- 'Enable remember browser feature for multi-factor authentication' checkbox: checked.
- 'Validity of browser fingerprint in hours. After remembering the browser user will not be challenged for 2nd factor authentication in the same browser for this duration.'': input field set to 8.
- 'Maximum number of browser a user can remember.'': input field set to 5.
- 'Default value of remember browser checkbox in the validate multi-factor page.'': checkbox: unchecked.
- 'Enable web authentication (FIDO2) based MFA' checkbox: checked.
- 'Enable email OTP for Multi-factor authentication' checkbox: checked.

A 'Save' button is located at the bottom right of the form.

3. Activate all multifactor Authentication Properties:

- Go to sys_properties table and search for “glide.authenticate.multi”

System Properties						
All > Name starts with glide.authenticate.multi!						
Name	Value	Type	Application	Description	Updated	Updated by
glide.authenticate.multi.factor	true	true false	Global	Enable Multi-factor authentication	2024-06-23 14:40:18	admin
glide.authenticate.multi.factor.browser.fingerprint.validity	8	integer	Global	Validity of browser fingerprint in hours...	2019-07-26 00:21:05	admin
glide.authenticate.multi.factor.clock_skew	10	integer	Global	Additional time in seconds for which the...	2015-07-30 15:45:25	admin
glide.authenticate.multi.factor.email.otp.enabled	true	true false	Global	Enable email OTP for Multi-factor authen...	2021-07-26 01:14:37	admin
glide.authenticate.multi.factor.remember.browser.enabled	false	true false	Global	Default value of remember browser checkbo...	2019-07-17 23:56:36	admin
glide.authenticate.multi.factor.remember.browser.max_sessions	5	integer	Global	Enable remember browser feature for multi...	2019-07-18 00:04:35	admin
glide.authenticate.multi.factor.remember.browser.max_time	3	integer	Global	Maximum number of browser a user can reme...	2019-07-26 00:20:55	admin
glide.authenticate.multi.setup.bypass.enabled				Number of times a user can bypass settin...	2015-05-12 14:28:47	admin

- Make sure to Enable multifactor authentication to user in user table

Users							
User ID	Name	Email	Active	Enable Multifactor Authentication	Created	Updated	
julius.reyes@example.com	Julius Reyes	julius.reyes@example.com	true	false	2026-09-13 22:34:57	2024-06-17 10:30:04	
hans.fischer@example.com	Hans Fischer	hans.fischer@example.com	true	false	2026-09-13 22:26:45	2024-06-17 10:30:04	
harding.asher@example.com	Harding Asher	harding.asher@example.com	true	false	2024-08-18 13:56:12	2024-06-17 10:30:04	
galileo			true	true	2024-06-23 14:50:03	2024-06-23 14:54:53	
gauss			true	false	2024-06-17 04:58:22	2024-06-17 04:58:22	
Test123	test123	test@yahoo.com	true	false	2024-06-16 15:36:34	2024-06-16 15:36:38	
test	test1	test1	true	false	2024-06-16 15:04:37	2024-06-16 15:04:30	

4. Configuring Multifactor authentication:

- Once user log back to another session it will pop up to create a multifactor Authentication to user.

Enable multi-factor authentication (MFA)

[More Information](#)

- 1 Download an authenticator app that supports Time Based One-Time Password (TOTP) on your mobile device.
- 2 Open the app and scan the QR code below to pair your mobile device



Or enter this code in your app:
XXXXXXXXXX [Copy](#)

3 Enter the code generated by the Authenticator app below

6-digit verification code

[Pair device and Login](#)


Postpone setup
Number of times MFA setup can be postponed is: 3

- Using above example user can use multifactor authentication application or OTP.



dev209613

Puneet

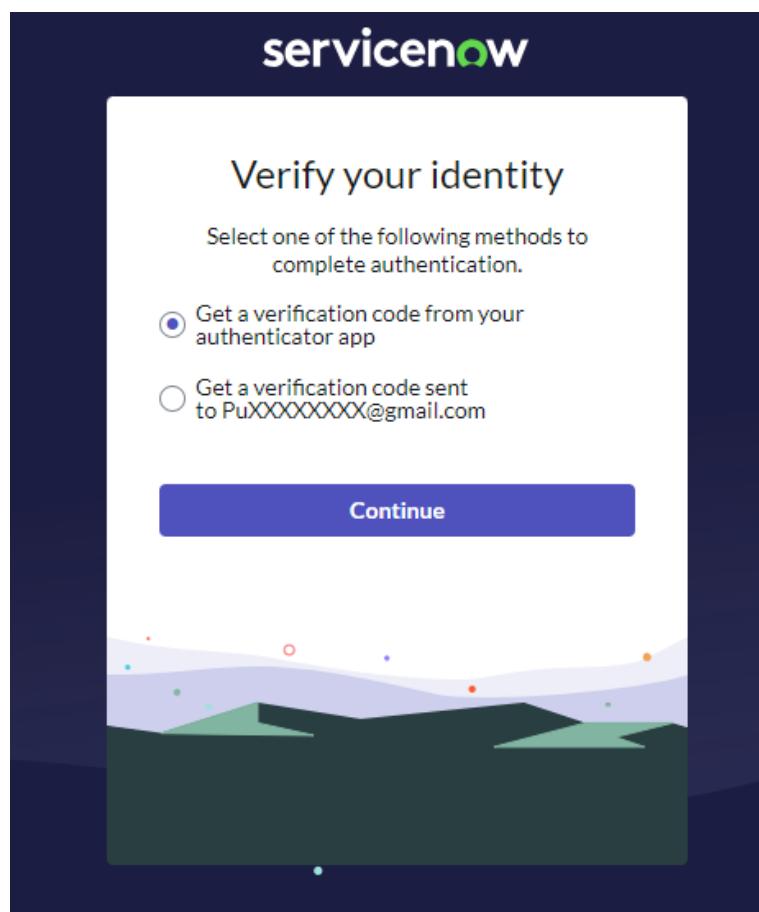


572 742 (16)

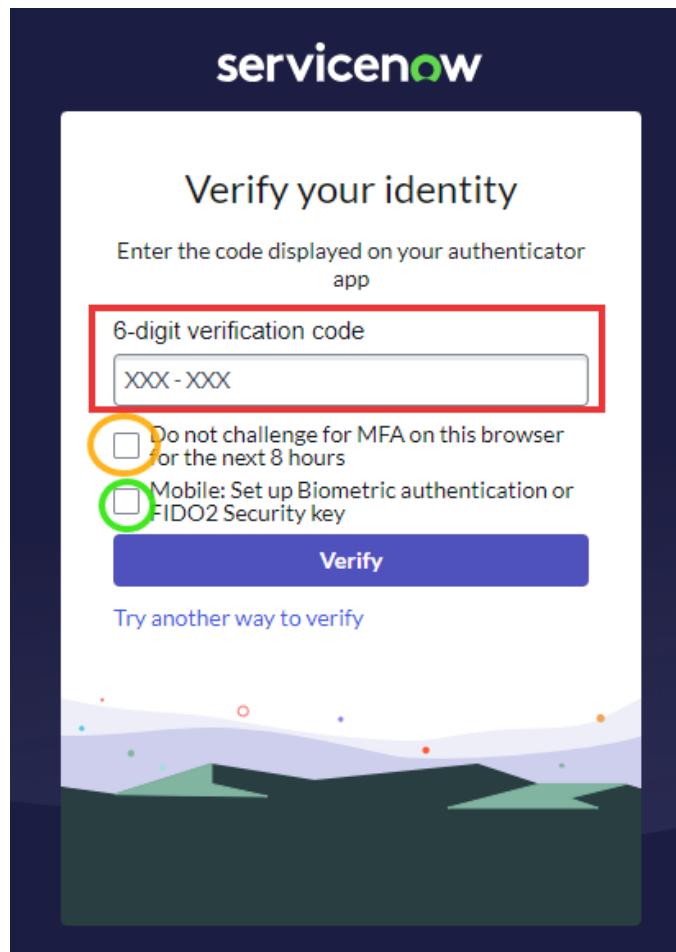
- As shown above You will receive TOPT from the authenticator application which will secure your instance more

5. Logging in with Multifactor Authentication:

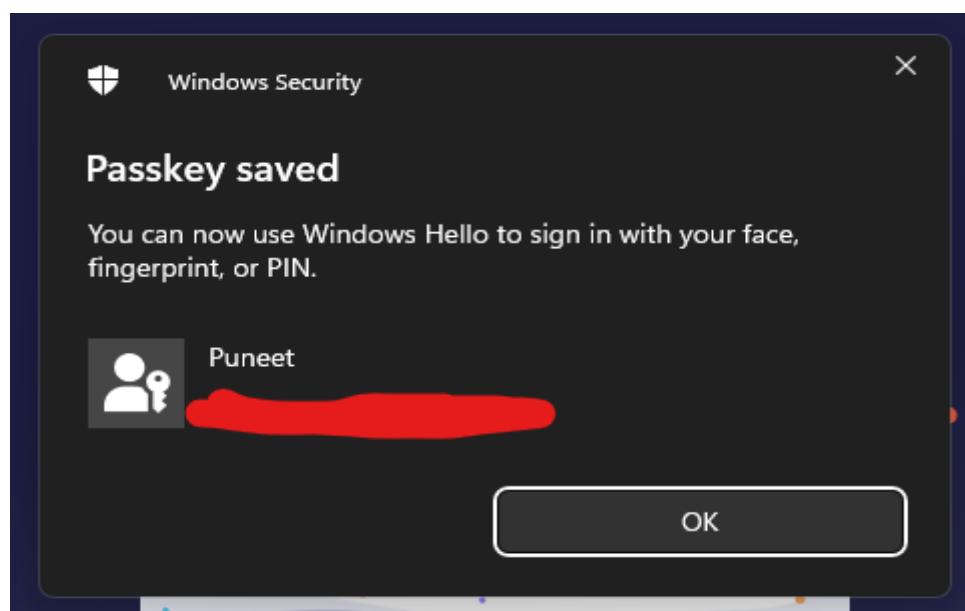
- Once user login It will provide opportunity to choose the authentication method if more then 1 type of authentication option are there



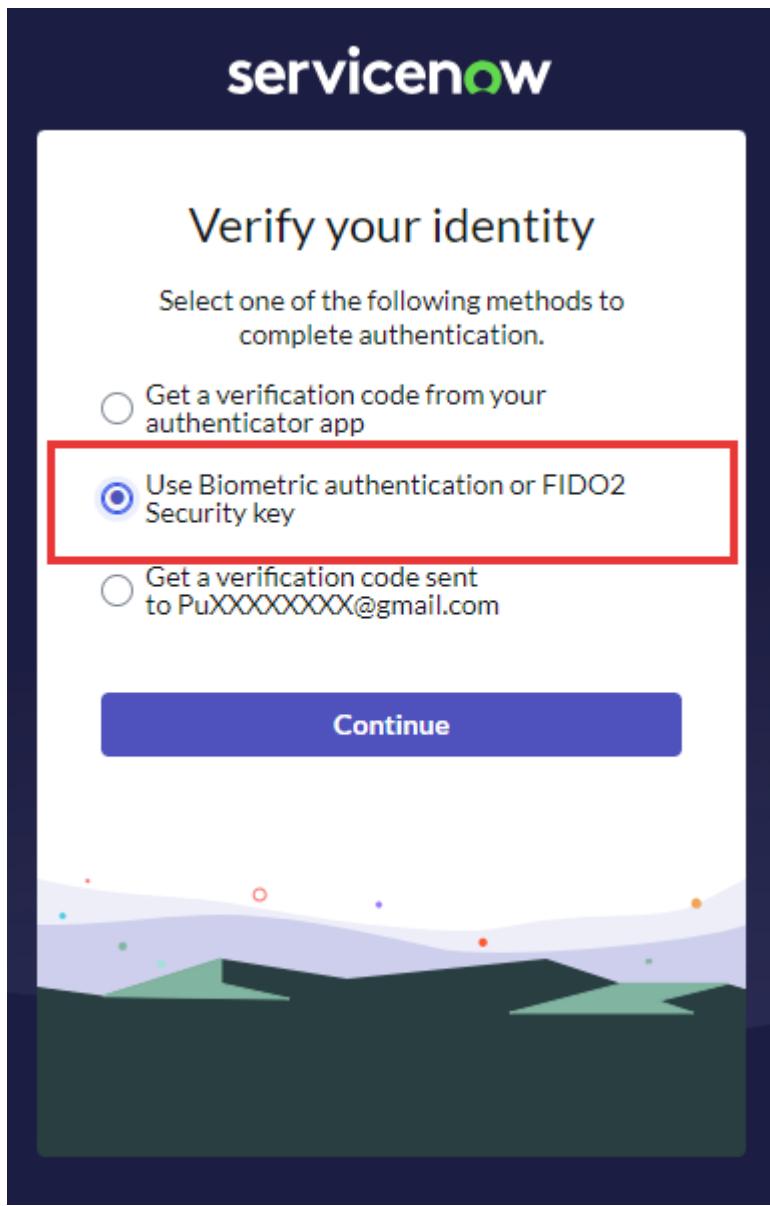
- Once you have selected type of authentication it will move to step to insert generated 6-digit code



- As shown in above screenshot it will ask you to skip the MFA for next 8hr and user can enable biometric or face unlock on their device based on the requirement.



- In case of enrolling device for Biometric MFA on that case new option will be visible to authenticate user



B. Testing the Implementation

1. **Test User Logins:**
 - Log in with a test user account to verify MFA prompts.
 - Ensure that the selected MFA methods are functioning as expected.
2. **Review Logs:**
 - Check Multi-Factor Authentication > Logs for any issues or errors during login attempts.

6. Best Practices

- **Backup Codes:** Provide backup codes for users in case they lose access to their MFA device.
- **User Training:** Educate users on the importance of MFA and how to use it effectively.

- **Regular Audits:** Conduct regular security audits to ensure compliance and effectiveness of MFA.
- **Policy Updates:** Keep MFA policies updated based on evolving security needs.

Multi-Factor Authentication (MFA) in ServiceNow: Implementation Guide

Table of Contents

1. Introduction
2. Benefits of MFA
3. Prerequisites
4. MFA Methods Supported in ServiceNow
5. Implementation Steps
 1. Enabling MFA in ServiceNow
 2. Configuring Identity Providers
 3. Setting Up MFA for Users
 4. Testing the Implementation
6. Best Practices
7. Troubleshooting
8. Conclusion

1. Introduction

Multi-Factor Authentication (MFA) enhances the security of user logins by requiring multiple forms of verification. Implementing MFA in ServiceNow ensures that only authorized users can access the system, thereby safeguarding sensitive data and applications from unauthorized access.

2. Benefits of MFA

- **Enhanced Security:** Reduces the risk of compromised credentials.
- **Compliance:** Helps meet regulatory requirements.
- **User Confidence:** Boosts trust by protecting user data.
- **Risk Mitigation:** Decreases the likelihood of security breaches.

3. Prerequisites

Before implementing MFA in ServiceNow, ensure the following:

- An active ServiceNow instance with admin access.
- A compatible identity provider (IdP) that supports MFA.
- Users' devices configured for receiving MFA tokens (e.g., mobile phones for SMS, authentication apps).

4. MFA Methods Supported in ServiceNow

ServiceNow supports various MFA methods, including:

- **SMS-Based OTP:** One-time password sent via SMS.
- **Email-Based OTP:** One-time password sent via email.
- **TOTP Apps:** Time-based One-Time Password applications like Google Authenticator or Authy.
- **Push Notifications:** Using apps like Duo Mobile for approval requests.

5. Implementation Steps

A. Enabling MFA in ServiceNow

1. **Navigate to the Multi-Factor Authentication Settings:**
 - Go to Multi-Factor Authentication > Settings in the ServiceNow instance.
2. **Enable MFA:**
 - Toggle the MFA option to enable it for your instance.
3. **Select MFA Methods:**
 - Choose the desired MFA methods (SMS, Email, TOTP, Push Notifications).

B. Configuring Identity Providers

1. **Integrate Identity Provider:**
 - Go to Multi-Provider SSO > Identity Providers.
 - Click New to add an identity provider.
 - Fill in the required fields such as Name, URL, and Client ID.
 - Configure the identity provider to support MFA.
2. **Configure SAML 2.0 Settings:**
 - Set up SAML 2.0 settings for authentication.
 - Ensure that the `AuthnContextClassRef` is set to require MFA.

C. Setting Up MFA for Users

1. **User Enrollment:**
 - Users need to enroll their devices for MFA.
 - Navigate to Self-Service > Multi-Factor Authentication Enrollment.
 - Follow the prompts to register the device (e.g., scan QR code for TOTP).
2. **Assign MFA Policies:**
 - Go to Multi-Factor Authentication > Policies.
 - Create and assign policies to users or groups to enforce MFA.

D. Testing the Implementation

1. **Test User Logins:**
 - Log in with a test user account to verify MFA prompts.
 - Ensure that the selected MFA methods are functioning as expected.
2. **Review Logs:**
 - Check Multi-Factor Authentication > Logs for any issues or errors during login attempts.

6. Best Practices

- **Backup Codes:** Provide backup codes for users in case they lose access to their MFA device.
- **User Training:** Educate users on the importance of MFA and how to use it effectively.
- **Regular Audits:** Conduct regular security audits to ensure compliance and effectiveness of MFA.
- **Policy Updates:** Keep MFA policies updated based on evolving security needs.

7. Troubleshooting

- **Device Sync Issues:** Ensure the user's device clock is synchronized for TOTP.
- **Connectivity Problems:** Verify that there are no network issues affecting SMS or push notifications.
- **User Enrollment:** Assist users in enrolling their devices correctly and troubleshooting common issues.

8. Conclusion

Implementing MFA in ServiceNow is a crucial step towards securing your organization's sensitive information. By following the outlined steps and best practices, you can ensure a smooth and effective deployment of MFA, enhancing the overall security posture of your ServiceNow instance.