

Uday Shivaswamy & Sadie Henry

Abstract

Self-service password reset enables your users to manage their passwords on their own. This reduces help desk costs, increases security, increases user productivity.

Azure Active Directory Project Planning Guide

**Self-service password reset**

Table of Contents

Contents

[Introduction 5](#_Toc508615598)

[Purpose of document 5](#_Toc508615599)

[Confidentiality statement 5](#_Toc508615600)

[What is self-service password reset? 5](#_Toc508615601)

[Current state of password reset 5](#_Toc508615602)

[Goals for Azure Active Directory Self-Service Password Reset Integration 6](#_Toc508615603)

[Confidentiality Statement 8](#_Toc508615604)

[Stakeholders and Sign-off 9](#_Toc508615605)

[Project Scope 10](#_Toc508615606)

[Prerequisites 10](#_Toc508615607)

[In scope 10](#_Toc508615608)

[Out of scope 10](#_Toc508615609)

[Business Use Cases 10](#_Toc508615610)

[Planning your Deployment 12](#_Toc508615611)

[General Planning 12](#_Toc508615612)

[Environments and project stages 12](#_Toc508615613)

[Licensing Considerations 12](#_Toc508615614)

[Planning for SSPR Enablement 13](#_Toc508615615)

[How password reset works 13](#_Toc508615616)

[Planning Password Authentication methods 14](#_Toc508615617)

[Changing administrator passwords. 15](#_Toc508615618)

[Important considerations for lock screen capabilities 16](#_Toc508615619)

[Planning for custom banned passwords 16](#_Toc508615620)

[Planning Deployment and Support 16](#_Toc508615621)

[Communications Planning 16](#_Toc508615622)

[Test Planning 18](#_Toc508615623)

[Support Planning 19](#_Toc508615624)

[Reporting Planning 19](#_Toc508615625)

[Implementing Your Solution 19](#_Toc508615626)

[Solution Components 19](#_Toc508615627)

[Timelines and environments 20](#_Toc508615628)

[Technical Requirements 20](#_Toc508615629)

[Change Communications 20](#_Toc508615630)

[Configuring Users and Licenses 20](#_Toc508615631)

[Ensure groups are created and populated 20](#_Toc508615632)

[Apply Licenses 20](#_Toc508615633)

[Configure the Azure AD Connect Service 21](#_Toc508615634)

[Configure the SSPR Service 22](#_Toc508615635)

© 2018 Microsoft Corporation.  All rights reserved.  This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice. You bear the risk of using it.   
Some examples are for illustration only and are fictitious. No real association is intended or inferred.   
   
This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes. You may modify this document for your internal, reference purposes

.

AZURE ACTIVE DIRECTORY

BUSINESS GUIDE

BUSINESS CASE FOR SELF-SERVICE PASSWORD RESET

# Introduction

## Purpose of document

The purpose of this document is to describe self-service password reset (SSPR) and how it will benefit our business. This document covers the business cases and goals for self-service password reset.

## Confidentiality statement

It is understood and agreed to that project plan may provide certain information that is and must be kept confidential. To ensure the protection of such information you should not disclose any part of this plan to anyone unless required to do so by law.

## What is self-service password reset?

Self-service password reset (SSPR) is a feature of Azure Active Directory that offers a simple means for IT administrators to empower users to easily reset their passwords and unlock their accounts. SSPR is designed to enable enterprises to decrease support costs, reduce user frustration and lost time, and increase user productivity and security. The system includes detailed reporting that tracks when users access the system, along with notifications to alert administrators to misuse or abuse.

## Current state of password reset

Replacing our current password reset infrastructure and migrating to Microsoft Azure Active Directory to manage self-service password reset will significantly reduce costs related to running, managing, and maintaining our current system.

<<this is an optional section in which you can detail your current state to help your stakeholders and decision makers understand the benefits specific to your enterprise of moving to SSPR. >>

<< Insert your summary text here. Eg: By moving to SSPR, we will save XX dollars in support costs, and NN people hours per week/year/incident due to password reset issues.>>

## Goals for Azure Active Directory Self-Service Password Reset Integration

Microsoft Azure Active Directory self-service password reset will benefit our business in the following ways:

|  |  |
| --- | --- |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Within_Your_Reach.png | **MANAGE COST**  Enabling SSPR with Azure Active Directory allows divestment of on premises infrastructures and reduces support costs by enabling users to reset their passwords on their own and reduces the cost of time lost due to lost passwords and lockouts. |
|  | **INTUITIVE USER EXPERIENCE**  Enabling self-service password reset provides users with the ability to reset their password from any device or locations. The intuitive, easy experience will allow users to get back to work faster and be more productive, while reducing their frustration. SSPR provides an intuitive one-time user registration process that ensures users will be able to rest passwords and unblock accounts on demand. Enterprises choose the information required for registration. |
| \\MAGNUM\Projects\Microsoft\Cloud Power FY12\Design\ICONS_PNG\Confidentiality.png | **FLEXIBILITY AND SECURITY**  Moving to Microsoft Azure Active Directory for self-service password reset enables enterprises to access the security and flexibility that a cloud platform provides. Administrators can easily change settings to accommodate new security requirements and then roll these changes out to users without causing disruption. |
| Magnifying glass | **ROBUST AUDITING AND USAGE TRACKING**  The auditing and usage tracking capabilities SSPR provides make it easy to see when users are resetting their passwords and ensure that business systems are stay secure. Auditing includes information on each step of the password reset process and is available from an API, which will enable us to import the data into a Security Incident and Event Monitoring (SIEM) system of choice. |
|  |  |

AZURE ACTIVE DIRECTORY

IMPLEMENTATION GUIDE

SELF-SERVICE PASSWORD RESET

How to use this guide

This step-by-step guide walks you through deploying and securing your application in a five-step process.



**1**

**Include**

Stakeholders

**2**

**Plan**

Your project

**3**

**Design**

Policies and integration

**5**

**Manage**

Your implementation



**4**

**Implement**

Your design

## Confidentiality Statement

It is understood and agreed to that project plan may provide certain information that is and must be kept confidential. To ensure the protection of such information you should not disclose any part of this plan to anyone unless required to do so by law.

## Stakeholders and Sign-off

The following roles will be involved in delivering this project. To see a full list of responsibilities and delivery items, see [Implementation Steps and Stakeholders](#_Implementation_Steps_and).

* Action Required:
  + SO = Sign-off on this project
  + R = Review this project and provide input
  + I = Informed of this project

|  |  |  |
| --- | --- | --- |
| Name | Area | Action |
| Enter name and email | IT Support Manager  A representative from the IT support organization who can provide input on the supportability of this change from a helpdesk perspective. | SO |
| Enter name and email | Identity Architect or Azure Global Administrator  A representative from the identity management team in charge of defining how this change is aligned with the core identity management infrastructure in the customer’s organization. | SO |
| Enter name and email | Business Owner  A representative colleague who can provide input on the user experience and usefulness of this change from an end-user’s perspective and owns the overall business aspect of the application, which may include managing access. | SO/I |
| Enter group alias for pilot group | End Users  The group of users for which SSPR will be implemented. They need proactive communications that SSPR is coming, how to register, and how to use it. [See sample communications.](#_Communications_Templates) | I |

## 

# Project Scope

## Prerequisites

The following are presumed to be in place prior to the beginning of this project.

* For hybrid environments, the Azure AD tenant has all user identities syncing from on-premises AD

## In scope

The following are in scope for this project:

**Enable self-service password reset**

* Applying licenses to users who will use SSPR
* Configuring SSPR for groups of users
* Configuring notifications
* Configuring SSPR using the Windows lock screen (Azure AD joined devices only)
* Enabling Azure AD Connect password write-back
* Configuring banned passwords – dynamic and custom lists

**Enable user registration**

* Configuring registration requirements
* Configuring SSPR Authentication methods for users

**Deployment and Support**

* Configuring end-user communications
* Working with audit logs
* Troubleshooting

## Out of scope

The following are out of scope of this project:

* Password replication to other LDAP or mainframe systems
* Synchronization of passwords across AD forests
* Applying password policies enforced through 3rd party apps
* Configuring Multi-factor authentication (MFA) and hardware token configuration
* Configuring SSPR using the Windows lock screen (Hybrid Azure Ad Domain joined devices)

## 

## Business Use Cases

The following table outlines the use cases to be implemented during this project.

|  |  |
| --- | --- |
| Area | Description |
| Access | SSPR portal is accessible from corporate and personal devices from any location (inside or outside the corporate network) |
| Auditing | SSPR registration and usage data is available to administrators to audit in near real time. |
| SSPR registration and usage data is downloaded into corporate systems at least every 29 days. |
| Governance | Lifecycle of user assignments to SSPR is defined and monitored[[1]](#footnote-2). |
| Security | Access to SSPR is controlled via user and group assignments. Only users who are enabled for SSPR can reset their own password. |
| Performance | Password change/reset propagation timelines are documented and monitored. |
| User Experience | Users are aware of SSPR capabilities and how to register. |
| Users are aware of how to self-manage their passwords. |
| Users are aware of browser compatibility. |
| Support | Users are aware of how to access support for SSPR issues. |

# Planning your Deployment

## General Planning

### Environments and project stages

Project stages are dependent on the environments that you have available. If you have a non-production Azure AD tenant, you can complete a proof of concept (POC) outside of your production environment if desired.

In the table below, document the Azure AD and AD environments and stages of your project.

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

### Licensing Considerations

We will need [Azure AD Licenses](https://azure.microsoft.com/en-us/pricing/details/active-directory/) for all users of SSPR. The number of objects in your directory and the features you wish to deploy will affect your licensing choices. While many features are included with Azure AD Free and Azure AD Basic, some features require Azure AD Premium (P1 or P2).

The following table describes some of the license requirements that may be relevant. For a full list of license requirements, click [here](https://azure.microsoft.com/en-us/pricing/details/active-directory/).

|  |  |  |  |
| --- | --- | --- | --- |
|  | Azure AD License Type | | |
|  | **BASIC** | **PREMIUM P1** | **PREMIUM P2** |
| Self-Service Password Reset for cloud-only users | Available | | |
| Self-Service Password Reset for hybrid users (with writeback) | Not available | Available | |

**Enterprise Mobility and Security (EMS) subscriptions:**

* EMS E3 includes P1
* EMS E5 includes P2

If you have an existing Enterprise Agreement or Server and Cloud Enrollment, you may already have Azure Premium. Check the details of your agreement.

### Best practices

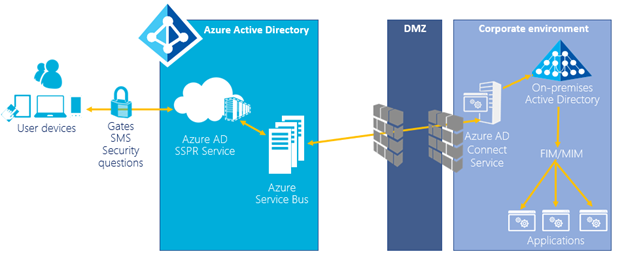
Here are a few best practices that other customers have used to ensure a successful rollout of SSPR.

* Before deploying SSPR, determine how many help desk calls happen per week/month and the average cost of each call. You can use this data post deployment to show the value SSPR is bringing to your organization.
* You can help users get registered quickly by deploying SSPR alongside another “popular app” in your organization. This will generate a large volume of sign ins and will drive up registration (if you have registration enforced).

## Planning for SSPR Enablement

### How password reset works

In all password reset scenarios in hybrid environments (environments where there is an on-premises Active Directory implementation and an Azure Active Directory implementation), the on-premises Active Directory is always the master for passwords.



When a user attempts to reset their password, they pass through the security gates and access the Azure AD SSPR Service, where they provide the new password. The new password is then written back to the master on-premises Active Directory via the Azure AD Connect Service.

For the password hashes to be synchronized to Azure Active Directory, password hash synchronization must be enabled in Azure AD Connect. When the password reset service detects that a synchronized user account is enabled for password hash sync, passwords are reset both the account’s on-premises and cloud password simultaneously.

To reset the password in the on-premises AD, Azure AD Connect must be able to communicate with the primary domain controller (PDC) emulator. If you need to enable this manually, you can connect Azure AD Connect to the PDC emulator. To understand password writeback in-depth, review [this](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-writeback) article.

#### Environments with multiple identity management systems

A picture containing text

Description generated with high confidence

If there are multiple identity management systems within an environment such as on-premise Identity managers like Oracle AM, SiteMinder, or other systems, then passwords written to the master Active Directory may need to be synchronized to the other systems using a sync engine such as PCNS plug-in with MIM (Microsoft Identity Manager). This is not covered by this deployment document. To find information on this more complex scenario, please see our [documentation](https://docs.microsoft.com/en-us/microsoft-identity-manager/deploying-mim-password-change-notification-service-on-domain-controller).

### Planning Password Authentication methods

These services enable administrators to configure the authentication methods that users can use to register and then prove their identity.

* Administrators configure the **Azure AD SSPR Service** with the available choices for end-users to provide their alternate credentials, and users access the service to register and to reset their passwords
* Administrators configure the **Azure AD Connect Service** to write back the passwords changes that occur in Azure AD back to the on-premises active directory.

In the following tables, record the values for the settings that you will need to plan to configure and provide typical values for those configurations.

**SSPR Configuration Values**

| Configuration | Recommendation | Vales to be configured |
| --- | --- | --- |
| Properties: Self-service password reset enabled (Pilot) | Identify the Azure AD security group to be used during the pilot and ensure all pilot members are a part of the group | Group: |
| Properties: Self-service password reset enabled | Identify the Azure AD security group or AD group synced to Azure AD to be used. If possible, we recommend selecting All. | Group: |
| Registration: Require users to register when signing in | Yes – this means that users will be asked to register when signing in and will help ensure that all users are registered | Value: |
| Registration: Number of days before users are asked to re-confirm their authentication information | 90-180 | Days: |
| Notifications: Notify users upon password reset | Yes – this ensures that your users will know whenever their password is reset through the SSPR flow | Value: |
| Notifications: Notify all administrators when other admins reset their password | Yes – this ensures that all admins are notified when an admin goes through the SSPR flow | Value: |
| Authentication methods: Number of methods required to reset | If possible, we recommend 2 to ensure a higher security posture | Values: |
| Authentication methods: Methods available to users | This may vary based on your requirements. We recommend choosing at least one more method than is required to reset. | Value: |
| Security questions: Number of questions required to register | If possible, we recommend that users register 5 questions so that they have flexibility | Value: |
| Security questions: Number of questions required to reset | We recommend 3 to ensure a higher security posture | Value: |
| Customization: Customize helpdesk link | Yes – this is extremely important for ensuring good user adoption. We recommend enabling this so that you can direct your users to the right place if they need help | Value: |
| Customization: Custom helpdesk email or URL | We recommend setting this value to the URL or email that your users usually use to get technical assistance | Value: |
| Write back passwords to on-premises AD | Yes, if your environment is hybrid (dependent on your subscription) | Value: |
| Allow users to unlock account without resetting password | Yes – this gives users more flexibility  (dependent on your subscription) | Value: |

### Changing/Resetting administrator passwords.

Administrator accounts are special accounts with elevated permissions. In order to secure them, the following applies to changing administrator passwords:

* On-premises enterprise administrators or domain administrators cannot reset their password through SSPR. They can only do this in their on-premises environment. Thus, we recommend not syncing on-prem AD admin accounts to Azure AD.
* A user administrator cannot reset the password of other administrators or a global administrator.
* An administrator cannot use secret Questions & Answers as a method to reset password. They must use phone/SMS only.

### Important considerations for lock screen capabilities

For users of Windows 10 computers to use SSPR, the computer must be joined to Azure Active Directory only (device must not be domain joined). [See our documentation](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-login) to learn how to enable this feature. This feature requires the Windows 10 Fall Creators Update (1709) or a newer Windows 10 version. The ‘Reset Password’ button can be enabled on the Windows 10 devices through Intune device configuration or a registry key (to be used for testing only). Note that password reset is not supported from a remote desktop.

## Planning Deployment and Support

An important part of planning deployment and support is ensuring that your end users are proactively informed about the service and how to register for it, can easily use the service, and are adequately supported if they run into problems.

### Communications Planning

The end user experience for SSPR registration and performing the password reset will be different from any existing toolset. There are multiple elements to planning your communication strategy. These include:

* Notifying users of upcoming and released functionality via
  + Email and other internal communication channels
  + Visuals such as posters
  + Executive live or other communications
* Determining who will customize and who will send the communications, and when.

Use the following table to plan your communications strategies. In the channels column, record the channels you will use for communications, including email, Yammer, Slack, intranet sites, etc.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Channels | Person customizing content | Person communicating | Date of communication |
| Initial communication to pilot users |  |  |  |  |
| Posters for pilot |  |  |  |  |
| Exec. comms. For pilot |  |  |  |  |
| Initial communication to all users for launch |  |  |  |  |
| Posters up for Launch |  |  |  |  |
| Exec. Comms. For launch |  |  |  |  |
| Post-launch follow-up communications |  |  |  |  |

#### Communications Templates

Below you will find customizable materials to use during rollout including email templates, posters, and table tents. You can adapt these materials for use in other communications channels as appropriate for your corporate culture.

### [Self-service password reset rollout materials](https://www.microsoft.com/download/details.aspx?id=56768)

### Test Planning

In this section, document how you will test during the pilot or other pre-production phases of your roll-out, as well as post-launch. Testing should ensure that your business use cases are covered. You can then use this table to record results. We have added a few cases based on the sample business requirements in this document, and on typical technical scenarios. You should add others specific to your needs.

|  |  |  |  |
| --- | --- | --- | --- |
| Business case | Device type | Expected result | Actual result |
| SSPR portal is accessible from within the corporate network | Corporate | Determined by your organization |  |
| Personal | Determined by your organization |  |
| SSPR portal is accessible from outside the corporate network | Corporate | Determined by your organization |  |
| Personal | Determined by your organization |  |
| Reset user password from browser when user is not enabled for password reset | Corporate | User will not be able to access the password reset flow |  |
| Personal |  |
| Reset user password from browser when user has not registered for password reset | Corporate | User will not be able to access the password reset flow |  |
| Personal |  |
| User signs in when password reset registration is enforced | Any allowed device | User will be prompted to register security information |  |
| User signs in when password reset registration has been completed | Any allowed device | User will not be prompted to register security information |  |
| SSPR portal is accessible when the user does not have a license | Any allowed device | Is accessible |  |
| Reset user password from lock screen after user has registered | Windows 10 AADJ or H+AADJ device | User can reset password |  |
| SSPR registration and usage data is available to administrators in near real time | NA | Is available via audit logs |  |

### Support Planning

While SSPR does not generally create user issues, it is important to have support staff prepared to deal with issues that may arise.

While a user administrator can change or reset the password for end users through the users & groups blade in Azure AD portal, it is generally better to help resolve the issue via a support process.

In the operational guide section of this document, create a list of support cases and their likely causes, and create a guide for resolution.

### Reporting Planning

###### Auditing

Audit logs for registration and password reset are available for 30 days. Therefore, if security auditing within a corporation requires longer retention, the logs need to be exported and consumed into a SIEM tool such as Splunk or ArcSight.

In the table below, document the backup schedule, the system, and the responsible parties. You may not need separate auditing and reporting backups, but you should have a separate backup from which you can recover from an issue.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Frequency of download | Target system | | Responsible party |
| Auditing backup |  | |  |  |
| Reporting backup |  | |  |  |
| Disaster recovery backup |  | |  |  |

# Implementing Your Solution

Now that you have planned your solution, you are ready to implement it.

## Solution Components

Implementation occurs in four stages:

* Configuring users and licenses
* Configuring Azure AD Connect Server for password write back
* Configuring the Azure AD SSPR service for registration and self-service
* Configuring banned passwords

## Timelines and environments

In the table below, copy in the information from planning environments

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

## Technical Requirements

## Change Communications

Begin implementation of the [communications plan](#_Communications_Planning) that you developed in the planning phase.

## 

## Configuring Users and Licenses

### Ensure groups are created and populated

Reference the [Planning password authentication methods](#_Planning_Password_Authentication) section and ensure the group(s) for the pilot or production implementation are available, and all appropriate users are added to the groups.

### Apply Licenses

The groups you are going to implement must have the Azure AD premium license assigned to them. You can assign them directly to the group, or you can use existing license policies (such as PowerShell or Group Based Licensing feature.)

#### Assigning licenses to groups

The groups that you have selected may already have licenses assigned.

**To check the assignment of licenses, perform the following steps:**

1. Access the [Azure portal](https://portal.azure.com) with an administrator account.
2. Select **All Services**, and in the **Filter** box, type **Azure Active Directory**, and then select **Azure Active Directory**.
3. Under **Manage**, select **Groups**, type the name of the group, and then select it.
4. In the group properties, select **Licenses**, and then ensure that the group has one of the following licenses assigned:
   * Azure AD Premium P1
   * Azure AD Premium P2
   * Enterprise Mobility + Security E3
   * Enterprise Mobility + Security E5
   * Microsoft 365 (Plan E3)
   * Microsoft 365 (Plan E5)

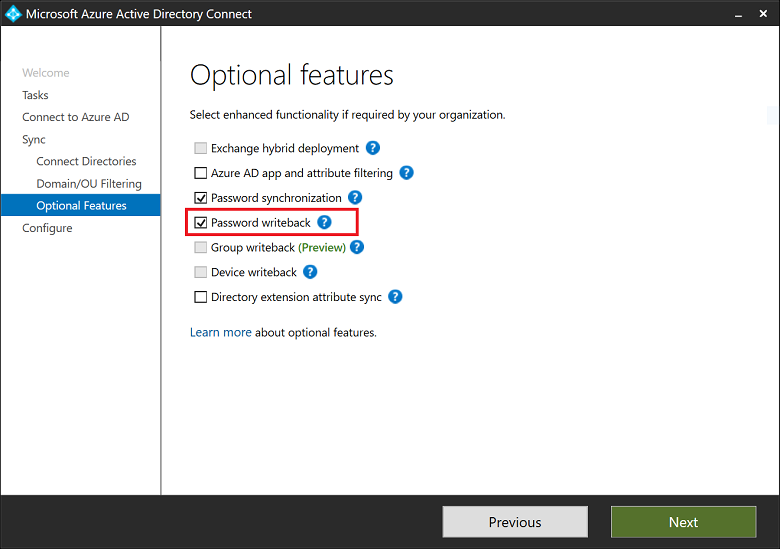
If one of those is assigned, you can move forward. If not, you will need to assign the license to the group(s).

**To assign licenses**

1. Access the [Azure portal](https://portal.azure.com) with an administrator account.
2. Select **All Services**, and in the **Filter** box, type **Azure Active Directory**, and then select **Azure Active Directory**.
3. Under **Manage**, select **Licenses**, and then **All Products**  
   All products available within your tenant are displayed.
4. Select one of the following licenses and then select **Assign.**
   * Azure AD Premium P1
   * Azure AD Premium P2
   * Enterprise Mobility + Security E3
   * Enterprise Mobility + Security E5
   * Microsoft 365 (Plan E3)
   * Microsoft 365 (Plan E5)
5. On the **Assign License** tab, select **Users and Groups**.
6. In the search box, type the name of the first group to be assigned the license, select the group, and then click the **Select** button at the bottom of the screen.
7. Repeat this process for each group

### Configure the Azure AD Connect Service

To configure password writeback:

1. To configure and enable password writeback, sign in to your Azure AD Connect server and start the **Azure AD Connect** configuration wizard.
2. On the **Welcome** page, select **Configure**.
3. On the **Additional tasks** page, select **Customize synchronization options**, and then select **Next**.
4. On the **Connect to Azure AD** page, enter a global administrator credential, and then select **Next**.
5. On the **Connect directories** and **Domain/OU** filtering pages, select **Next**.
6. On the **Optional features** page, select the box next to **Password writeback** and select **Next**. 
7. On the **Ready to configure** page, select **Configure** and wait for the process to finish.
8. When you see the configuration finish, select **Exit**.

The password-write back feature is now on and SSPR will now work from the portal or from the Windows lock screen.

#### Enable SSPR in Windows

**Windows 10 devices**: Users can use Windows 10 Azure AD joined devices to perform SSPR. No further SSPR configuration is required. Follow [this article](https://docs.microsoft.com/en-us/azure/active-directory/device-management-hybrid-azuread-joined-devices-setup) to ensure Windows 10 devices are Azure AD joined.

### 

### Configure the SSPR Service

#### Enable Groups for SSPR

1. Access the [Azure portal](https://portal.azure.com) with an administrator account.
2. Select **All Services**, and in the **Filter** box, type **Azure Active Directory**, and then select **Azure Active Directory**.
3. On the Active Directory blade, select **Password reset.**
4. In the properties pane, select **Selected**.  
   Note: if you want all users enabled, Select All.
5. In the **Default password reset policy** blade, type the name of the first group, select it, and then click **Select** at the bottom of the screen, and select **Save** at the top of the screen.
6. Repeat this process for each group.

#### Configure the Authentication methods

Reference your planning from the [Planning Password Authentication Methods](#_Planning_Password_Authentication) section of this document.

1. Select **Registration**, under **Require user to register when signing in**, select **Yes**, and then set the **number of days before expiration**, and then select **Save**.
2. Select **Notification**, and configure per your plan, and then select **Save**.
3. Select **Customization**, and configure per your plan, and then select **Save**.
4. Select **On-premises integration**, and configure per your plan, and then select **Save**.

|  |  |  |  |
| --- | --- | --- | --- |
| Environment | Environment URL | Project stage | Start/Finish date |
| Non-production |  | POC-Configuration | / |
|  | POC-Testing | / |
| Production |  | Configuration | / |
|  | Testing | / |
|  | Pilot | / |
|  | General Availability | / |

# 

# Operational Document

## Required Roles

|  |  |  |
| --- | --- | --- |
| Personas | Roles | Azure AD Role (if required) |
| Level 1 Helpdesk |  | Password admin |
| Level 2 Helpdesk |  | User admin |
| SSPR Admin |  | Global admin |

## 

## Support Case Scenarios

To enable your support team success, you can create an FAQ based on questions you receive from your users.

The following table contains common support scenarios.

|  |  |
| --- | --- |
| Scenarios | Description |
| User does not have any registered authentication methods available | A user is trying to reset their password but does not have any of the authentication methods that they registered available (i.e. they left their cell phone at home and can’t access email) |
| User is not receiving a text or call on their office or mobile phone | A user is trying to verify their identity via text or call but is not receiving a text/call. |
| User cannot access the password reset portal | A user wants to reset their password but is not enabled for password reset and therefore cannot access the page to update passwords. |
| User cannot set a new password | A user completes verification during the password reset flow but cannot set a new password. |
| User does not see a Reset Password link on a Windows 10 device | A user is trying to reset password from the Windows 10 lock screen, but the device is either not joined to Azure AD, or the Intune device policy is not enabled |

You may want to create a cheat sheet of support steps specific to your organization. In that cheat sheet, you should include information on:

* which groups are enabled for SSPR
* which authentication methods are configured.
* the access policies related to on or of the corporate network.
* troubleshooting steps for common scenarios

The following table contains general troubleshooting steps for the most common scenarios.

|  |  |
| --- | --- |
| Scenarios | Resolution |
| There is an issue with the service, password writeback, or other issue not specific to a user (Admins / Tier 3) | [Troubleshooting Self-Service Password Reset](https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-troubleshoot) for service Administrators |
| Error message: We could not verify your account User does not have any registered authentication methods available | Direct the user to register at <https://aka.ms/ssprsetup>  Additional information: [End user: how to register for password reset](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-reset-register) |
| Error Message: Your account is not enabled for Password Reset | Ensure that the SSPR service is configured  Ensure that the user is in the group that is enabled for SSPR  Ensure that the user is licensed for SSPR |
| Error Message: We've detected that your user account password is not managed by Microsoft. As a result, we are unable to automatically reset your password | Ensure that password writeback is enabled in Azure AD Connect |
| Error Message: We're sorry, but we cannot reset your password at this time. This is due to a temporary connectivity issue, so if you try again later, resetting your password may succeed. | Ensure outbound port 443 is enabled for the Azure Ad Connect machine  Check errors/warnings in the event logs for the Azure AD Connect machine  Re-enable password writeback  Check for firewall or software that kill idle connections |
| User is not receiving a text or call on their office or mobile phone | Ensure that the user is registered.  Ensure that the user phone number in the system matches the phone number the user has access to.  Ensure that this method is configured in the service. |
| User cannot access the password reset portal | Determine if the user is on or off the corporate network.  Determine if the user is enabled for SSPR through group membership. |
| User cannot set a new password | Verify password policies  Ensure that the user is registered.  Ensure that the user phone number in the system matches the phone number the user has access to.  Ensure that this method is configured in the service. |
| User does not see a Reset Password link on a Windows 10 device | Ensure that the device is Azure AD joined (and is not domain joined to a on-premises domain)  Ensure that the Intune device policy is enabled for the device to enable password reset  Ensure the user is not in a Remote desktop session (this use case is not supported) |

### Expected SLA

|  |  |
| --- | --- |
| Scenarios | Results |
| SLA for Azure AD | Azure AD guarantees at [least 99.9% availability](https://azure.microsoft.com/en-us/support/legal/sla/active-directory/v1_0/) of the Azure Active Directory Basic and Premium services. |
| SLA for support case resolution | Depends on the support tier |
| Business Impact if outage occurs | <Add business risk here> |

## Auditing

|  |  |
| --- | --- |
| Scenarios | Results |
| Security | <how will you look for bad actors trying this, or lockouts> |
| Log in monitoring | <optional: how will you look for various aspects of user risk> |
| Access and Control | < optional: who has access to the audit logs> |
| Operational Monitoring | < optional: who monitors regularly> |
| Business Metrics/Usage | < optional: when will alerts be raised> |

## 

## Helpful Documentation

[Getting started with password reset](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-getting-started)

[Password reset overview](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-overview)

[Password reset deep dive](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-how-it-works)

[Password reset deployment guide](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-best-practices)

[Password reset from Windows lock screen](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-login)

[Password policies](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-policy)

[Password reset experience customization](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-customize)

[Deploy password reset without requiring end-user registration](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-data)

[Password reset reporting options](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-reporting)

[How to manually reset a user’s password](https://docs.microsoft.com/azure/active-directory/active-directory-users-reset-password-azure-portal)

[Licensing requirements for password reset](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-licensing)

[Password reset overview and instructions](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-writeback)

[Password reset troubleshooting](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-troubleshoot)

[Password reset FAQ](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-faq)

[End user: how to reset your password](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-update-your-own-password)

[End user: how to keep your password secured with password reset](https://docs.microsoft.com/azure/active-directory/active-directory-secure-passwords)

[End user: how to register for password reset](https://docs.microsoft.com/azure/active-directory/active-directory-passwords-reset-register)

# 

1. Requires Azure Active Directory Premium 2, or EMS 5 licenses. [↑](#footnote-ref-2)