Your expert infrastructure partner

Microsoft Partner
Microsoft

Gold Datacenter
Gold Cloud Platform
Gold Cloud Productivity
Silver Small and Midmarket Cloud Solutions
Silver Enterprise Mobility Management

Modern Authentication

Statement of Work

<CompanyName>

Document Version: 1.0,

Commercial Owner:

Solution Owner:

Quote Number:

Confidentiality

Summary

As part of <CompanyName> audit requirements there is a requirement to enable multi-factor authentication, to comply with this task. <CompanyName> has decided to implement Microsoft Azure Active Directory MFA. As part of this implementation it has been agreed to enable the <CompanyName> staff to use Windows Hello for business, along with the Microsoft Azure Active Directory Self Service Password Reset platform to help reduce the number of support tickets while ensuring that the environment is secure.

This scope includes:

1. examination of the state of Active Directory as it relates to authentication, as well as the current state of the configuration of Intune and MFA.
2. Upgrade of the Active Directory server on premises and the backup in Azure. This involves a schema update which will allow support of the new authentication information which will be stored in Active Directory and Azure Active Directory. The relevant information will be synchronised between directories using the Active Directory Connect service. Updating Active Directory is a relatively safe process, and a recent backup is used for roll-back if required.
3. Documentation will include a description of how the service is enabled, what the staff experience is for turning it on and using it, as well as common troubleshooting activities.
4. Hand over to internal support will involve a workshop to walk through documentation and follow up Teams session to encourage retention of the information.

Solution overview

The first phase of this engagement will be to perform a health check of the efic.gov.au domain, along with the <CompanyName> Azure Active Directory tenant, this will include reviewing and documentation of the current replication processes both between the existing domain controllers and between the efic.gov.au domain and the <CompanyName> AAD tenant. Any issues found during this phase will be communicated to all parties to agree on any corrective actions which might arise.

To successfully deliver the modern authentication solution it is required that an existing domain controller is uplifted to Windows Server 2019. Vigilant.IT recommends that the existing domain controller in Azure be replaced with a Windows Server 2019 OS, with little impact for the business, while the Domain Controller that is located in Export House will require an outage depending upon how existing systems are linked to it.

Before any action is performed on the Domain Controllers Vigilant.IT will perform a health check to ensure that there are no active replication issues. As part of this health check, it will review the current state of the AAD MFA environment, and document any changes which are required to implement the project successfully.

Once the domain controllers have been replaced, a new certificate template will be created on the efic.gov.au (This is the existing On-Premises domain) certificate authority which will be then made available to the domain controllers to facilitate Kerberos authentication from Azure Active Directory joined workstations to existing domain member servers.

For the staff who already have MFA enabled Vigilant.IT will enable Windows Hello for Business for there accounts. For the remaining staff Vigilant.IT will be creating collateral to educate the <CompanyName> team the process to enable both MFA and SSPR on their account along with ensuring Windows Hello for Business is enabled.

> Vigilant.IT recommends the use of the Microsoft Authenticator application on iOS and Android devices with push notification enabled as the preferred Multi-Factor Authentication tool.

As this project will be directly impacting all staff at Export Finance, Vigilant.IT recommends that an education package is devised that will include a quick reference guide, using the following links to configure both of the systems.

- https://aka.ms/setupmfa
- https://aka.ms/ssprsetup

As this is an integral part of getting access to corporate data outside of the <CompanyName> network, it is important that the mobile phone that is enrolled for MFA is with the staff member at all times.

The transition to support team will be based upon the quick reference guide that is provided staff while including references to how the policies are applied to the end-users. There will also be a hand over session performed by the engineer who has implemented the solution.

Commercials

Task	number of days	Rate/Day	Cost (ex GST)
Domain health check	1	$2,150	$2,150
Domain controller upgrades	4	$1,800	$7,200
Certificate template creation and issuance to domain controllers	2	$1,800	$3,600
Creation of documentation	2	$1,800	$3,600
Hand over to support teams	1	$2,150	$2,150
Total			**$18,700**

Assumptions and Constraints

The project will proceed with the following identified assumptions. Any further assumptions or constraints that are identified as the project progresses will be subject to a change control and an impact analysis, which may affect the cost and timescales of the project. Where these changes were not reasonably identifiable by Vigilant.IT then the customer will bear additional costs if any.

Ref.	Description
A1	There is full disclosure of all relevant information by <CompanyName>.
A2	Stakeholders will be available to Vigilant.IT for workshops or meetings.
A3	<CompanyName> can receive signoff in a timely manner.
A4	Access to the site and areas within the site required to perform tasks outlined herein will be made available to Vigilant.IT staff in a timely manner.
A5	Appropriate working environment will be available to Vigilant.IT staff, such as seating and desks.
A6	Requested documentation and information will be provided to Vigilant.IT within a timely manner.
A7	Any decisions from parallel projects that could impact this proposal will be communicated to Vigilant.IT without delay.
A8	<CompanyName> will communicate to Vigilant.IT, prior to project commencement, any project risks or dependencies that may affect this engagement
A9	<CompanyName> will ensure that all relevant aspects of the Work Health and Safety Act and its regulations will be complied with in relation to the workplace in which Vigilant.IT resources are required.
A10	That security passes, should they be required, will be arranged in a timely fashion.

A11	Only the works specified in this document form the initial proposed engagement. Any additions to the scope or the proceeding implementation will be an additional cost.
A12	The scope of works has been clearly communicated and agreed with all <CompanyName> staff involved in this proposal.
A14	Suitably qualified <CompanyName> staff will be available throughout the engagement for the purposes of requirements gathering and knowledge transfer.
A15	Relevant environment access is granted to Vigilant.IT resources.
A16	Any timescales or plans presented in this document assume that <CompanyName> provides any required information and fulfils its other obligations as described in a timely manner. If <CompanyName> fails to meet these obligations, Vigilant.IT may adjust the timeline or costs with notice to <CompanyName> to address the delays or failures to meet obligations.
A17	Vigilant.IT standard templates are acceptable for this engagement.
A18	<CompanyName> will arrange and co-ordinate all meetings and handover workshops, ensuring appropriate staff are present.
A19	All the works are to be conducted during normal Business Hours (9:00am to 5:30pm, Monday to Friday, excluding local Public Holidays). Any out of business hours work will be considered as a project variation.
A20	All submitted changes by Vigilant.IT to any documents will be deemed accepted by <CompanyName> unless written changes or modifications are made within 5 working days after reception of said documents.

Change Management Process

For any changes (see definition of change below) to this Statement of Work (SoW), <CompanyName> must submit the request in writing to the Vigilant.IT Solution Owner for this project (see title page). The Solution Owner will evaluate the request and advise options given project constraints (time, budget, resources).

Signature Page

Accepted by <CompanyName>	**Accepted by Vigilant.IT**
Signature	Signature
Leon Gort	
Name	Name
Head of ICT	
Title	Title
Date	Date

Document History

Document Control

The following table describes each version release of this document and references any changes made to it, by whom and when for each specific release.

Version	Date	Author	Comments
0.1			
0.2			
1.0			

Understanding the version numbers

- Releases prior to version 1.0 are for internal drafts / review only.
- Version 1.0 is the first client release ready for distribution outside of Vigilant.IT
- Each review completed shall increase the version number by 0.1
- Each acceptance/rejection of changes made by the authors following a review increases the version number by 0.1
- The current document version is shown on the cover page and in the table above.

Document Distribution

The current version has been distributed to the following recipients:

Recipient Name	Email Address	Title