VeroGuard with VeroLink Set-up Guide

Version 1.2 ● 12 October 2021

VeroGuard Systems

VeroGuard Systems – Melbourne, Australia – Phone: +61 3 9558 3090

Email: - info@veroguard.com.au

Table of Contents

Table of Figures

1 Introduction

1.1 Purpose

This document discusses how to prepare your environment for integration with VGS.

1.2 Scope and intended reading audience

This Guide is primarily aimed at personnel who will be configuring and administering VeroGuard on an on-premises Active Directory environment.

This guide provides information on setting up your Active Directory environment so that your systems can subsequently be integrated with VGS.

1.3 Initial checks

Before starting, ensure you meet the following **minimum requirements.**

1. A Domain Controller running Windows Server 2016 or higher.
2. An Active Directory Domain Services (AD DS) environment, with or without Active Directory Federation Services (AD FS). Azure Active Directory Domain Services is **not** supported by this version of VGS.
3. An active internet connection.
4. Each PC which will be used with VGS must have:
    a. Windows 10 installed (version 1803 or higher); and
    b. Bluetooth installed and enabled (VeroGuard also supplies a USB BT adaptor with the VeroCard).

1.4 Summary of this guide

In summary, this guide will take you through the following steps:

a) Selecting a computer or VM on which to install VeroLink (section 2).
b) Configuring your domain controller for use with VeroLink and deciding whether to allow VeroLink to control administrative accounts (section 3).
c) Installing VeroLink on the selected computer or VM (section 4).
d) Configuring workstation for use with VeroLink and logging in using a VeroCard (section 5).

Section 6 also provides some further technical details about how VeroLink works.

2 Select a machine for VeroLink installation

2.1 About VeroLink

VeroLink is a .net core application designed to support VeroCard's access to Active Directory (AD) services.

VeroLink is configured to run as a Windows service on the Microsoft Windows 10 (or higher) or Microsoft Windows Server 2016 (or higher) operating systems. To work properly, the VeroLink machine must be a part of the client's domain and have access to the client's Active Directory.

Interacting with Active Directory, VeroLink (on behalf of the user) performs two main operations: changes the user's password and obtains user account data.

Once VeroLink is up and running, it tries to establish a connection to the VeroGuard server and remains connected indefinitely until its connection is terminated. If the connection is lost, VeroLink tries to reconnect the VeroGuard server.

2.2 Summary of requirements

As noted above, VeroLink must be installed on a computer or virtual machine (VM) which is running either Microsoft Windows 10 (or higher) or Microsoft Windows Server 2016 (or higher). As also noted above, it must be installed on a computer or VM that is part of a local domain.

In addition to this, the computer or VM on which VeroLink is installed must be able to access, at minimum:

a) port 389 of the primary domain controller of that domain; and
b) port 443 at wss.veroguard.online (i.e. over the internet).

To satisfy the above requirements while maximizing security, we recommend installing VeroLink on a computer or VM which is on a separate VLAN and which has access only to the above noted ports for the above noted hosts (plus any other ports / hosts required for maintenance).

2.3 Identify VeroLink machine

In subsequent steps, you will need to grant permissions to the machine account of the computer or VM on which VeroLink has been installed. Accordingly, at this point you should identify the computer or VM on which you will later install VeroLink (taking into account the above requirements) and make a note of its host name.

However, it is suggested that you do not install VeroLink until you have completed the following section dealing with domain controller configuration.

3 Domain Controller Configuration Process

3.1 Background

In order for VeroGuard to function correctly, VeroLink must be able to and access and cycle users' passwords. To do this, it must be given certain permissions on the domain's primary domain controller.

VeroGuard will only be able to control passwords of users who have been added to the appropriate security group. By default, VeroLink will also only be able to control users who are not administrators.

If you wish to have VeroLink control administrators' passwords you will need to take extra steps (see 3.4. below)

The next two sections describe how to create the appropriate security group, add users to it and give VeroLink the necessary permissions to access and cycle passwords for those users.

3.2 Set up OU and Security Group

While logged in to a domain controller on the relevant domain:

a) open Active Directory Users and Computers;
b) create an Organisational Unit (OU) name "VeroControlledOU" at the root of the domain tree. This will be the OU into which the new Security Group will be placed, then
c) create a new Security Group named " VeroControlled", into which you will later place users who receive VeroCards.

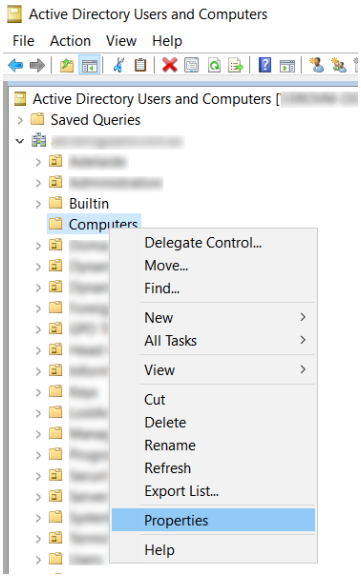
3.3 Give permissions to VeroLink

At this point, you must identify each OU in which there are users who will be using a VeroCard (see above for default names). VeroLink must be given the appropriate permissions to read and cycle passwords for each such OU.

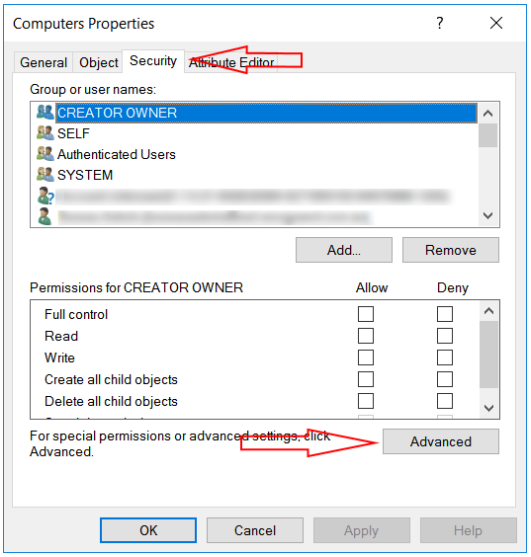
VeroGuard will not actually be able to manage the passwords of users in an OU simply because VeroLink has been given access to change passwords in that OU. To enable password changes for a particular user, the additional step of adding the user to the VeroControlled security group must be taken. See figure 3 below.

For each relevant OU:

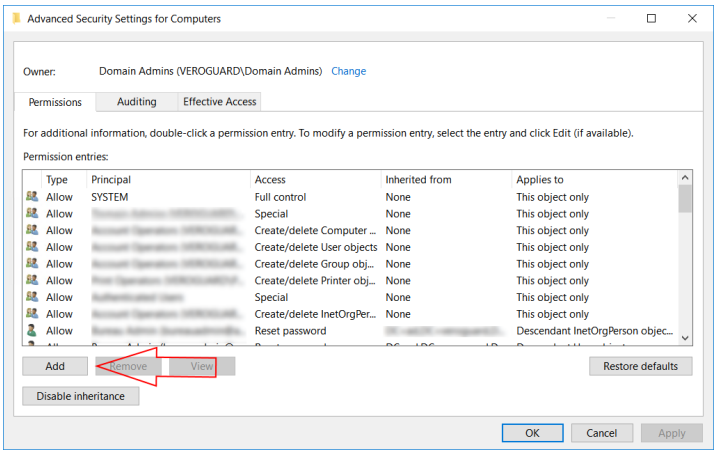
a) In Active Directory Users and Computers, right click on the OU and from the drop-down menu, select “Properties”:



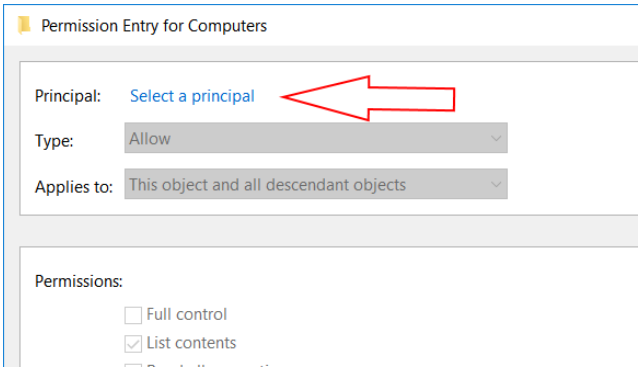
b) In the resulting “Properties” window, select the “Security” tab and click the “Advanced” button at the bottom of that tab:



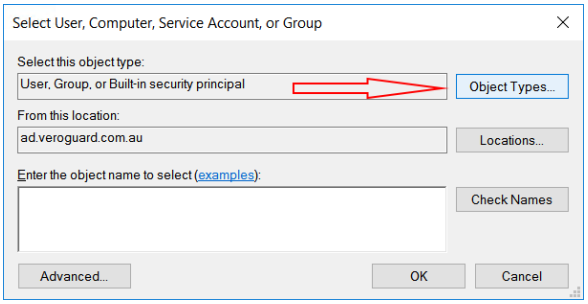
c) The “Advanced Security Settings” windows should open on the “Permissions” tab. On this tab, click the “Add” button:



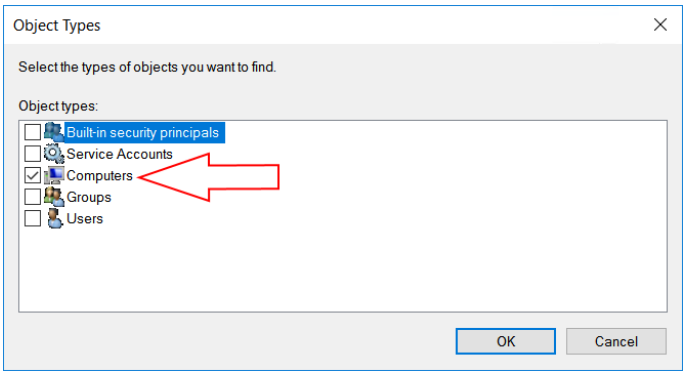
d) On the resulting “Permission Entry” window, click “Select a Principal”:



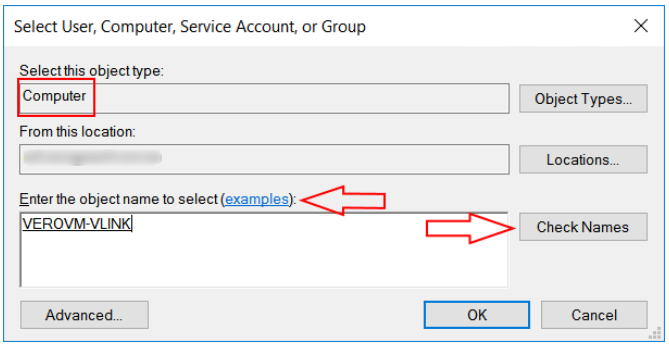
e) In the resulting “Select User, Computer, Service Account or Group” window, click the “Object Types” button:



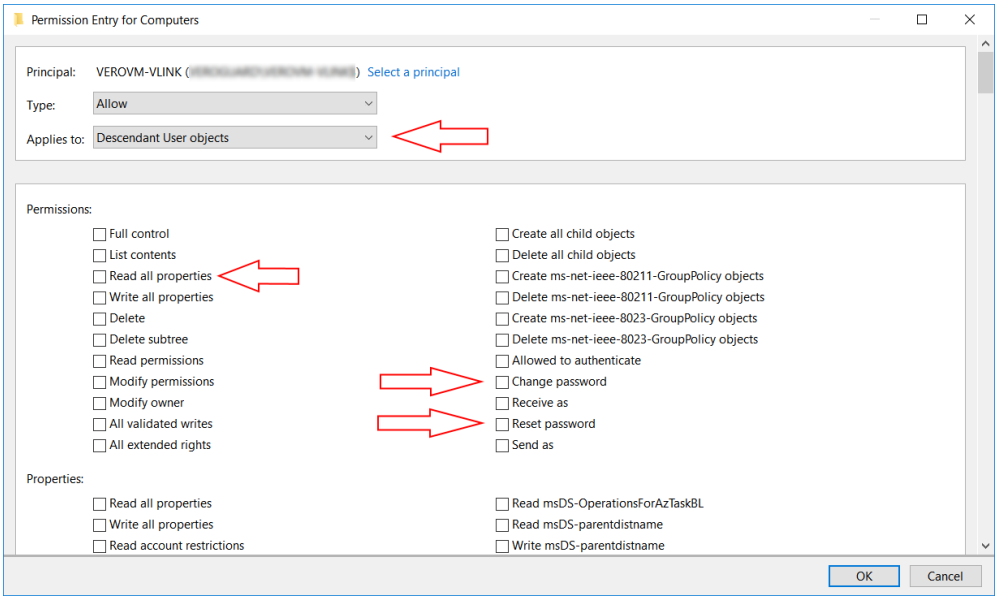
f) In the resulting “Object Types” window, select “Computers”. You may also de-select all other object types, to make your search easier:



g) After doing this, click the “OK” button. You will return to the “Select User, Computer, Service Account or Group” from step e) above. However, in the “Select this object type” box, the word “Computer” should now be included (as shown below). In the “Enter the object name to select” box, enter the name of the computer or VM on which VeroLink will be installed (in the illustration below, the name “VEROVM-VLINK” is used as an example). After entering the name, click the “Check Names” button. If you have entered a correct and unique name, it will be automatically underlined. You may then click the “OK” button:



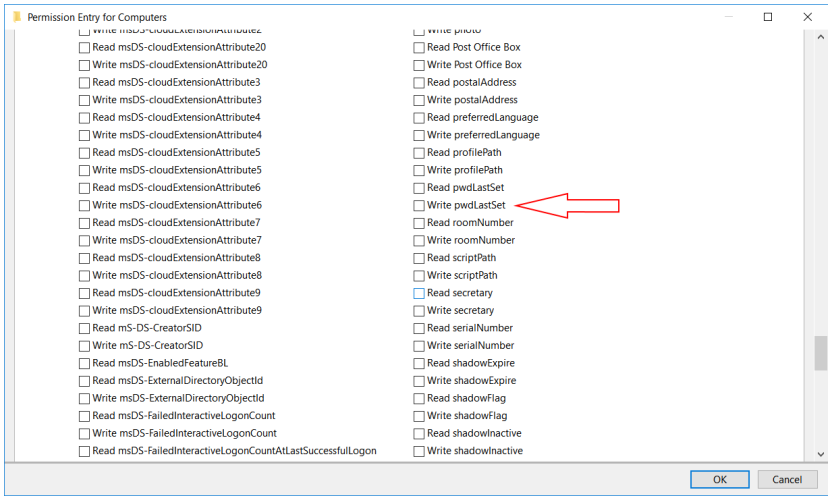
h) You should now be presented with a “Permission Entry” window similar to the image below:



i) On the “Applies to” drop-down menu, select “Descendant User Objects”. The list of permissions and properties will then change.

j) Check the “Read All Properties”, “Change Password” and “Reset Password” boxes under “Permissions” (note that change and reset password are two separate permissions, both of which are required).

k) Scroll down until you locate the “Write pwdLastSet” permission and check the box for it as well:



l) Click “OK” on this window and all other open windows until you have returned to the main “Active Directory Users and Computers” window. You have now applied the necessary permissions for VeroLink to manage non-administrative users.

3.4 Choose whether to allow control of administrative users

At this stage, you must decide whether you will allow VeroLink to control passwords for users who are members of the “Domain Administrators” or “Enterprise Administrators” security groups. If you decide to do so, you will need to take further steps to enable VeroLink to control such users.

Below, two different methods are described. Each has its benefits and its drawbacks. You should carefully consider if either method suits your requirements.

*Depending on your infrastructure and security environment, either or both of the below methods may introduce some risk to IT infrastructure. These risks are further explained below. If you are not certain that this risk can be mitigated, we recommend you **not** allow VeroLink to control administrative users, as that is the safer course of action. To do this, simply skip over the steps described in sections 3.5 or 3.6 below.*

3.5 Admin control Method A: create admin user

The first way to allow VeroLink to control administrative users is to create a new user just for this purpose, make that user a Domain Administrator and give that user’s credentials to the VeroLink application. VeroLink will then route requests for change of administrative passwords via this new user.

The advantages of this method (as compared to Method B below) are:

- The machine account of the device on which VeroLink is installed does not itself have any administrative rights.
- Accordingly, if an attacker is able to compromise this machine account, they will not be able to use it to manipulate any administrative user accounts.

The disadvantages of this method (as compared to Method B below) are:

- An extra Domain Administrator user must be created and its credentials must be recorded and stored. This creates a potential window for those credentials to be lost or stolen.
- User accounts (such as the one being created for this purpose) may generally be more vulnerable to compromise than machine accounts (such as the machine account on which VeroLink is installed). If this particular user account is compromised, the attacker will have direct and extensive control over the relevant domain.

If you would like to use this method to have VeroGuard manage administrative users, you should:

a) create a new user in the relevant domain;
b) give that user a strong password;
c) set the user's password so that it does not need to changed at next logon and never expires;
d) for each OU containing administrative users that you need to be controlled by VeroGuard, give this user all the same permissions that you provided to the VeroLink machine account in step h) of section 3.3.

Make a note of the user's name and password, as these will be required in subsequent steps.

3.6 Admin control Method B: VeroLink rights to AdminSDHolder

The second way to allow VeroLink to control administrative users is to give the VeroLink machine account certain permissions over the "AdminSDHolder" container. The AdminSDHolder container holds the security descriptor templates applied to members of certain protected groups, such as Domain Administrators and Enterprise Administrators.

Accordingly, if VeroLink is given the necessary permissions over this container, it will be able to change the passwords of anything in this container – including administrative users.

The advantages of this method (as compared to Method A above) are:

- No extra accounts are required to be created, potentially reducing the overall attack surface.
- As the VeroLink machine account is used, it is not necessary to record any administrative credentials outside of AD, potentially narrowing the window for credential theft.
- Machine accounts may generally be less vulnerable to compromise than user accounts.

The disadvantages of this method (as compared to Method A above) are:

- The VeroLink machine account will have the permissions to change passwords for *all* administrative users and all other objects inside the AdminSDHolder container.

- While VeroLink will not manage passwords for accounts that are not in the VeroControlled security group, if an attacker is able to gain control of the VeroLink machine account they will be able to change passwords for any and all administrative users in the relevant domain. This may allow the attacker to defeat attempts at remediation.

If you would like to use this method to have VeroGuard manage administrative users, you should simply give the VeroLink machine account all the same permissions over the AdminSDHolder container that you provided to it over OUs in step h) of section 3.3

3.7 Add users to VeroControlled

Before proceeding, please ensure that, for any user which will be migrated to VeroGuard, the users has: (a) the AD attribute sAMAccountName populated within their AD account ("sAMAccountName" must be unique for each user on the domain); and (b) the "User cannot change password" attribute ticked (i.e. their ability to change their password turned off). See illustration below.

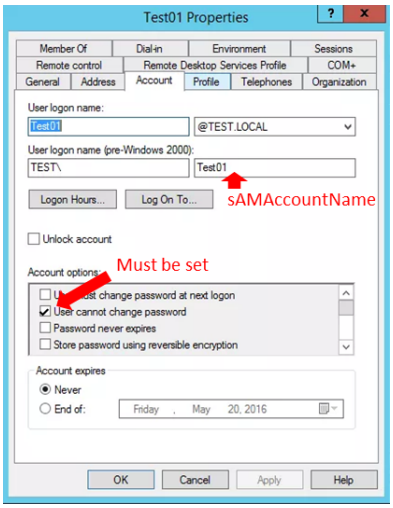


Figure 1. *Example of correctly configure user properties for migrating user.*

At this point, add each user who will use a VeroCard to the "VeroControlled" security group.

Only users who are added to this group can use VeroCards to log in to a Windows PC on the domain.

In the event you wish to override VeroGuard, you are advised to keep at least one Enterprise or Domain Admin account(s) outside of the VeroControlled group and keep the account's password securely stored.

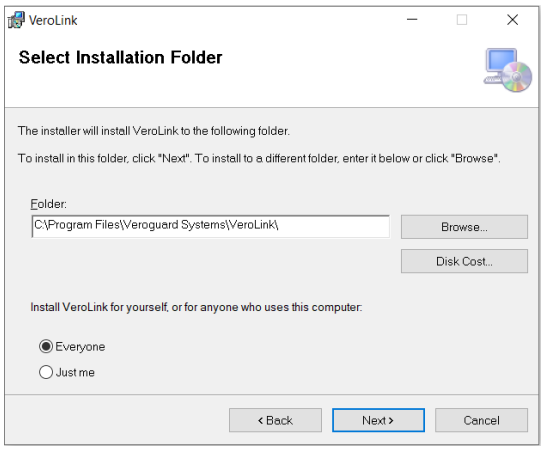
4 VeroLink Installation process

4.1 Installation of package

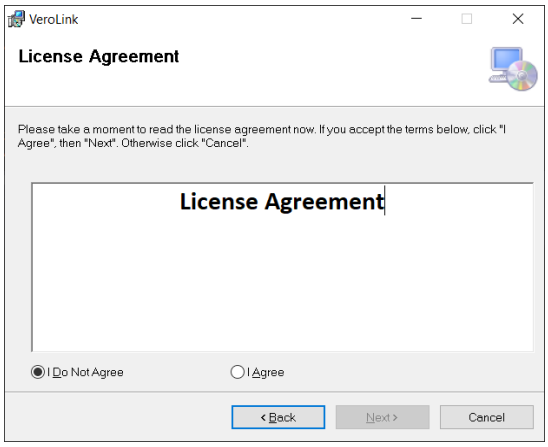
Once you have set up a computer or VM as suggested in earlier sections, copy the provided VeroLink installer to that computer or VM.

Locate the VeroLink installer and execute it by double clicking on it, then follow the steps provided by the Setup Wizard below:

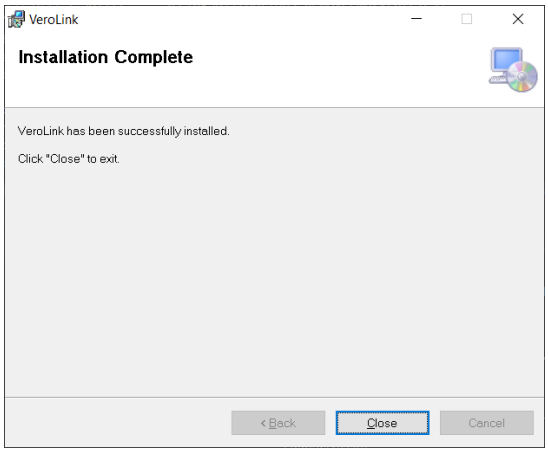
You will need administrative privileges to install VeroLink. If you are not logged in as an administrator of the relevant computer, you can right click on the installer, choose "Run as Administrator" from the drop-down menu, then provide your administrative credentials when prompted.



Accept the License Agreement to procced:



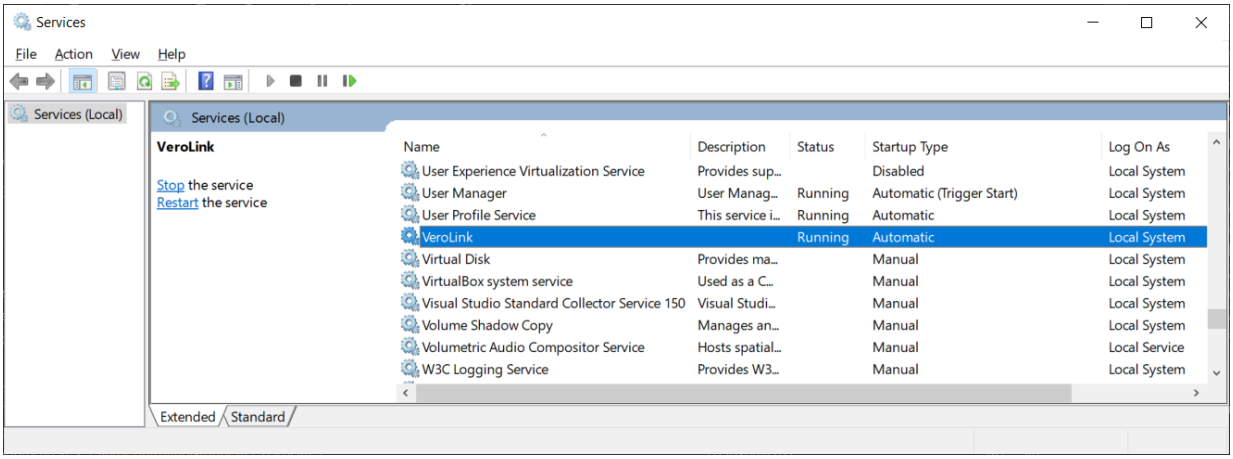
Finally, the last screen will be displayed:



4.2 Verify installation

The above process installs the VeroLink as a windows service and starts it in a 'LocalSystem' account context.

After the installation process is complete, open Windows Service Manager and ensure the VeroLink service is installed and running:



4.3 Customise installation

While still logged on to the computer or VM on which VeroLink is installed:

a) go to the directory into which you installed VeroLink (by default `C:\Program Files\Veroguard Systems\VeroLink`).

b) In this directory, find the file named "appsetings.Initial.json". Open this file in a text editor such as Notepad. Open the file this using the "As Administrator" option, otherwise you will be unable to write changes.

c) In the file find the following parameters, which by default will be set to "****", with the following details:

   i. "Origin" – set this to your internal domain (e.g. "int.company.com").

ii. "ClientSecret" – set this to the initial client secret provided to you by VeroGuard (NB this will be replaced with a new randomly generated secret created by the VeroLink client after initial use).

iii. "LdapServerConnection" – set this to the FQDN of your primary domain controller (e.g. "dc1.int.company.com").

iv. "LdapSearchBaseDn" – set this to the DN of base OU of the location at which you want VeroLink to be able to search, in LDAP Data Interchange Format (e.g. if your domain is "int.company.com" and you would like VeroLink to search the whole domain, this would be set to "DC=int,DC=company,DC=com").

v. "MemberOf" – set this to the DN of the VeroControlled security group in LDAP Data Interchange Format (e.g. " CN=VeroControlled,OU=Security Roles,DC=int,DC=company,DC=com").

d) **Optional steps – allow changes of administrative users' passwords** : If you wish to control administrative users with VeroGuard using Method A described above (this step is not necessary for Method B), then:

i. Firstly, ensure you have followed the steps in section 3.5of this document. If not, go back and follow those steps.

ii. Open the "appsetings.Initial.json" in a text editor such as Notepad. Open the file this using the "As Administrator" option, otherwise you will be unable to write changes.

iii. Find the following text in the file: "LdapAdminUserDn": "****".

iv. Replace "****" on that line (excluding the quotation marks) with the name of the admin user you created in section 3.4, using the format "username@domain.tld".

v. Find the following text in the file: "LdapAdminUserPassword": "****".

vi. Replace "****" on that line (excluding the quotation marks) with the password for the above administrative user.

e) Restart the VeroLink Service

You have now completed initial VeroLink setup.

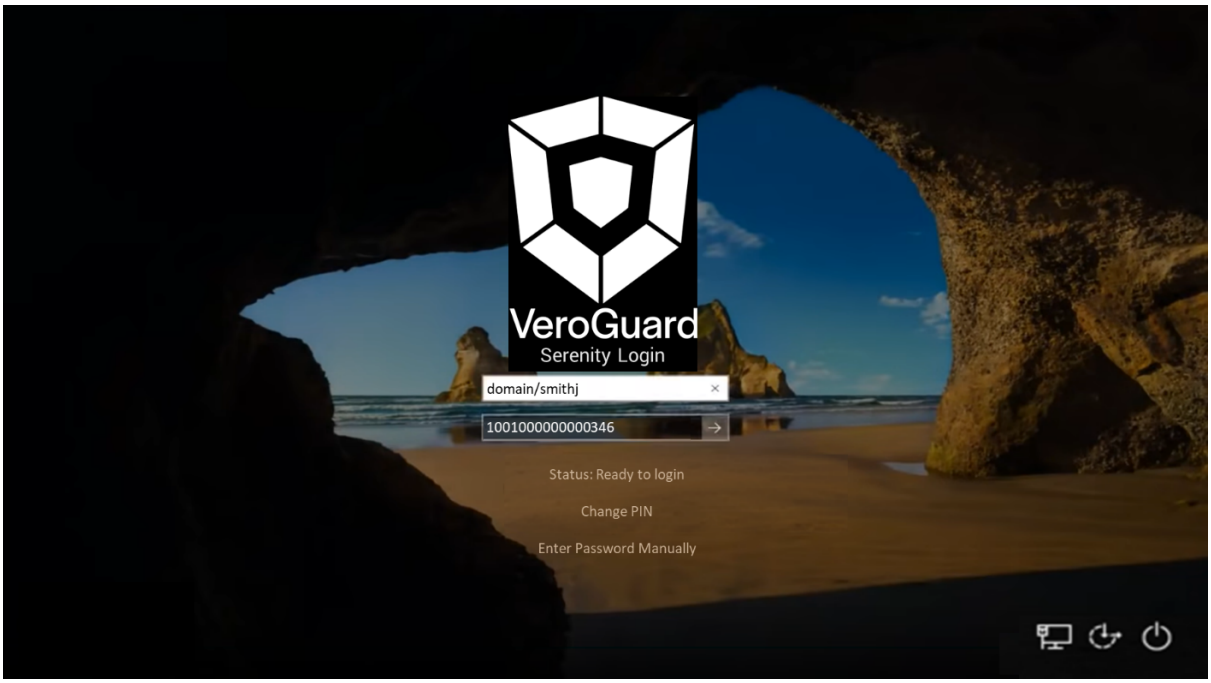
5 Workstation setup

5.1 Install the Serenity Windows client

Each PC which will be accessed via VeroGuard will need to have the Serenity Credential Manager installed on their devices to enable secure authentication and communications with VeroCards. Serenity can be downloaded from support.veroguard.com.au/downloads.

Please make sure you select "Serenity AD"

Once this is completed the User Log in Screen will change to the VeroGuard screen.



5.2 Initial Login with a VeroCard

When logging in with a VeroCard the first time the user will be prompted to set their PIN. VeroCards support PIN numbers from minimum 4 to maximum 12 digits.

When initially logging on with a new VeroCard on to a PC:

a) Turn on the PC and ensure the Bluetooth and network connections are activated.
b) Log out (Win L) and hit any key for the login screen to appear.
c) Turn on your VeroCard (press the button on the left side).

d) Wait for the PC to detect the VeroCard. Once it is ready, its Terminal ID number will be displayed in the dropdown box. If other VeroCards have been detected in the vicinity you may need to select your card from the dropdown box.
e) Once selected click the right arrow or press enter.
f) The VeroCard will now go through an activation process including setting of the user PIN.
g) Follow the screen prompts on the PC and the VeroCard.

All future logins must be via the VeroCard.

To login on with a VeroCard the first time, a user must be connected to the network. Full end user guide can be found at support.veroguard.com.au

6 Further Information about VeroLink

6.1 Where to find certain key files and folders

The following default are used by the installer for the following folders and file names:

Executable file name	`VeroLink.exe`
Windows Service Name	`VeroLink`
Default Folder name	`C:\Program Files\Veroguard Systems\VeroLink`
Default Log files	`C:\logs\verolink.log` `C:\logs\werolink_error.log`

6.2 VeroLink up-date mechanism

VeroLink has a self-updating feature that checks for available updates every time it starts. VeroLink sends updates over the web socket channel. If a newer version is present in the Update folder inside the application's working directory, VeroLink is updated and restarted.

6.3 Dive deeper into the inner workings

VeroLink is self-sufficient (published using a self-contained deployment mode) and does not require any other third-party services and databases to operate. The VeroLink software runs over a secured channel (TLS 1.2) and its key parameters are stored in the appsettings.Initial.json file.

Under the hood: At startup, VeroLink encrypts its key parameters and creates the appsetting.Production.json file in an encrypted format. After starting VeroLink, the appsetings.Initial.json file with the original unencrypted settings should be moved from its working directory and stored in a safe place for future use.

6.4 Configuration file internals

Below is an example of the initial VeroLink configuration file (appsetings.Initial.json) (see **Figure 2**). This file is designed to be modified with your environment's values. VeroLink uses this file during its initial start-up and encrypts specified key values. The result of this operation is a Production configuration file which is used at each subsequent start of the VeroLink software (see **Figure 3**).

```
{
    "Logging": {
        "LogLevel": {
            "Default": "Information",
            "Microsoft": "Warning",
            "Microsoft.Hosting.Lifetime": "Information"
        }
    },
    "UseCCStore": true,
    "ClientCertificateFile": "<Your-Client-Certificate-Filename>",
    "ClientCertificatePassword": "<Your-Client-Certificate-Password>",
    "ClientCertificateIssuerName": "<Client-Certificate-Issuer-Name",
    "ModifiableProperties": "Description,DisplayName,MobilePhone,PostalAddress,PrimaryEmail,GivenName,SN",
    "EncryptedParameters": "ClientId,WSServerUrl,ClientSecret,Scope,BaseApiUrl,LdapServerConnection,LdapPort,LdapAdminUserDn,LdapAdminUserPassword",
    "AllowedHosts": "*",
    "AppSettings": {
        "ReconnectIntervalInSeconds": "5"
    },
    "LBTargetGroup": "A",
    "Origin": "Client-web-site.com",
    "ClientId": "<Client-Id-ProvidedBy-Veroguard>",
    "ClientSecret": "<Client-Secret-Password-ProvidedBy-Veroguard>",
    "Scope": "Client-Scope-ProvidedBy-Veroguard",
    "WSServerUrl": "<Verolink-Server-Name>",
    "CustomerId": "<Customer-Id-ProvidedBy-Veroguard>",
    "ClientBufferInBytes": "8192",
    "BaseApiUrl": "https://api.veroguard.online/veroauth",
    "ConfigurationName": "veroguard.online",
    "LdapServerConnection": "<Customer's-LDAP-Server>",
    "LdapPort": 389,
    "LdapServerTimeoutInSeconds": 10,
    "LdapUseSsl": false,
    "LdapVerifyCert": false,
    "UseAnonymous": false,
    "LdapAdminUserDn": "<Customers-LDAP-Username>",
    "LdapAdminUserPassword": "Customers-LDAP-Password",
    "LdapServerBaseDn": "<Customers-LDAP-Distinguished-Name>",
    "LdapObjectClass": "top;person;organizationalPerson;user",
    "MemberOf": "VeroControlled"
}
```


Figure 2. *Initial VeroLink configuration file example*

The Production configuration file has encrypted key values:


```
{
    "Logging": {
        "LogLevel": {
            "Default": "Information",
            "Microsoft": "Warning",
            "Microsoft.Hosting.Lifetime": "Information"
        }
    },
    "UseCCStore": true,
    "ClientCertificateFile": "<Your-Client-Certificate-Filename>",
    "ClientCertificatePassword": "<Your-Client-Certificate-Password>",
    "ClientCertificateIssuerName": "<Client-Certificate-Issuer-Name",
    "ModifiableProperties": "Description,DisplayName,MobilePhone,PostalAddress,PrimaryEmail,GivenName,SN",
    "EncryptedParameters": "ClientId,WSServerUrl,ClientSecret,Scope,BaseApiUrl,LdapServerConnection,LdapPort,LdapAdminUserDn,LdapAdminUserPassword",
    "AllowedHosts": "*",
    "AppSettings": {
        "ReconnectIntervalInSeconds": "5"
    },
    "LBTargetGroup": "A",
    "Origin": "Client-web-site.com",
    "ClientId": "CfDJ8KmaUXUU7vNFqmQRqjQIJu_NrQzNFbzvAOxW1emDuXAyHBwTGV5hRE7pEJoKzQvfYbdKVEqvqs3GGTswDev-b-861MnGuyf6h2k7WWcjffd58mUqVJQccUHFzApx2I2sGg",
    "ClientSecret": "CfDJ8KmaUXUU7vNFqmQRqjQIJu_iQpma-m8VRkhB8Pd5zV3cB5cUm-OCdylk15dZsQg4q1fKnSEITzGfoUSFknLklvJ2ShIBrpl9AgCcFSv9ZOC5Xw-84nmRq0Vcb7NBrBTvcMi88KwnLdtDpxLBqcgrqPrUsj8FwNEJL3b_tBg0Xphs",
    "Scope": "CfDJ8KmaUXUU7vNFqmQRqjQIJu8YLLjbT29Fg7Cd_rAlli2smaC_QF6CCH5uEO0gLgYW83PhjFf8YBPuedVRuae0LUpqf3V3t6nFF81dn0avGCs7IyPryqUq8uIvHivZEMg5KQ",
    "WSServerUrl": "CfDJ8KmaUXUU7vNFqmQRqjQIJu-werl9Z_mstR-LNui5dHIJDAmZOVY1hKLIibvAhlMjYD3-cv2Cfbh59Z5Wy3Sa2tSBJARlALY8r2Gxu-GbphxBKsY6NXkWu8lHdX7zCkj06Yr3Qh0F0IEN93pLa7vzaeE",
    "CustomerId": "<Customer-Id-ProvidedBy-Veroguard>",
    "ClientBufferInBytes": "8192",
    "BaseApiUrl": "CfDJ8KmaUXUU7vNFqmQRqjQIJu9sYxdbOCoGXH_Qq5T8A30FYMuSmwpowN--EzuKJklu5A8OJOHyxxI1Ipw18iAycpkpfLZ7J7IFQUvRm55RPNlMQXtwL6G6uzicmRuChIB7EawvUPTT5UroTEgmgD7lE48kKNaPEL_lGwlnQuUojq2O",
    "ConfigurationName": "veroguard.online",
    "LdapServerConnection": "CfDJ8KmaUXUU7vNFqmQRqjQIJu8mEHgDNWNkRwJgJ082H1-1jfYEc9O4GxOzItqVCza0mExazJ316ROK987-ykxUky4Spxe-PaNou_isRM8NlxT5pEXkNHJXLwNET9Q5bHDWRq-Ltgb6ZIV_gxO4IIX_RT8",
    "LdapPort": 389,
    "LdapServerTimeoutInSeconds": 10,
    "LdapUseSsl": false,
    "LdapVerifyCert": false,
    "UseAnonymous": false,
    "LdapAdminUserDn": "CfDJ8KmaUXUU7vNFqmQRqjQIJu819NgCNpNbvw8upE4v0CJd-L40zfjgngWW2jTRMEksxLmG9NlizZG3cpQAOZaZboi0QSc1D8azxPaFdwxN3giGEKFCuzJJfmtUUeYiqs9AodxE-geiRPH2VhMVMS2QEzc",
    "LdapAdminUserPassword": "CfDJ8KmaUXUU7vNFqmQRqjQIJu_9nbxzYQadn22Q9-cAYNDPdA7z6VEOgEHArzoZw-Qj725BhsPa-1U32XlLBNUKWE5hN3axdMT6KOKODdCz12RhutD2tmDSCkHZWw6AodTXCA",
    "LdapServerBaseDn": "<Customers-LDAP-Distinguished-Name>",
    "LdapObjectClass": "top;person;organizationalPerson;user",
    "MemberOf": "VeroControlled"
}
```


Figure 3. *VeroLink Production Configuration file example*

This file is automatically generated by VeroLink and has only specified amount encrypted parameters.

The Microsoft asp.net runtime unique machine key that distinguishes one computer from others is used to encrypt these three parameters (see https://docs.microsoft.com/en-us/aspnet/core/security/data-protection/introduction?view=aspnetcore-5.0 for details).

Initial encryption occurs the first time the application is launched. An initial configuration file with unencrypted parameters must be provided in the `appsetting.Initial.json` file. After running the application and encrypting the settings in the `appsettings.Production.json` file, the original `appsettings.Initial.json` file is no longer needed for the application and should be moved from the application working folder to any safe location at the Customer's discretion.

If the application needs to be reinstalled or moved to another computer, the original, unencrypted `appsettings.Initial.json` file must be used to recreate the encrypted version of the current `appsetting.Production.json` configuration.

If the original unencrypted `appsettings.Initial.json` file is lost OR any encrypted data (such as Active Directory data or the VeroLink server URL) has changed, you can recreate it using appsettings.Production.json. To do this, follow these steps:

1. *Rename `appsettings.Production.json` to `appsettings.Initial.json`.*
2. *Replace the encrypted key values with unencrypted values that can be requested from Veroguard.*
3. *Restart the application.*
4. *Move the `appsettings.Initial.json` file to any secure location.*