HIDEEZ Cyberark Authentication Integration

Technical documentation

Name of Company: Hideez Group Inc.

Website: https://hideez.com

Name of Product: HideezKey

Version: ST101/ ST102

Date: 27.11.2018

PARTNER SOLUTION OVERVIEW

The user authenticates using the HTTPS web-based access to the PVWA system (the CyberArk authorization system is configured as a client of the RADIUS server). The user enters the basic credentials (Login and Password) using HideezKey as a reliable hardware password storage. The CyberArk system, after checking and confirming the base user accounts, makes a request to the remote RADIUS server, which is configured in conjunction with the one-time password generator system, and requests the user to confirm the OTP confirmation code. The user using the HideezKey enters a confirmation code. In case of incorrect verification of the code, access is denied to the user. Upon successful verification, the RADIUS server confirms the authenticity of the user to the CyberArk PVWA system. PVWA allows the user inside in accordance with the rights granted by the CyberArk system.

KEY BENEFITS

1) Hideez Key - The Last Mile in Identity and Access Management

2) Why Hideez Password Keeper?
   A) Protects against digital identity theft, phishing, credential stuffing, and account Take-overs
   B) Only password keeper for digital and physical access
   C) Outsmart vulnerabilities of other industry players
   D) Increased productivity of employees
   E) Compatible with existing infrastructure
   F) Minimized risk of Human Error

3) Why?
   Stolen credentials are used to commit fraud on an enormous scale through Account Takeover (ATO) or credential stuffing attacks. This presents a huge problem for businesses with employees online. Data breaches can compromise your internal documents and processes, your sensitive customer data and your financials.

4) Trends:
   USABILITY is the top of the list
   Passwords
   Blockchain
   Multifactor of Authentication

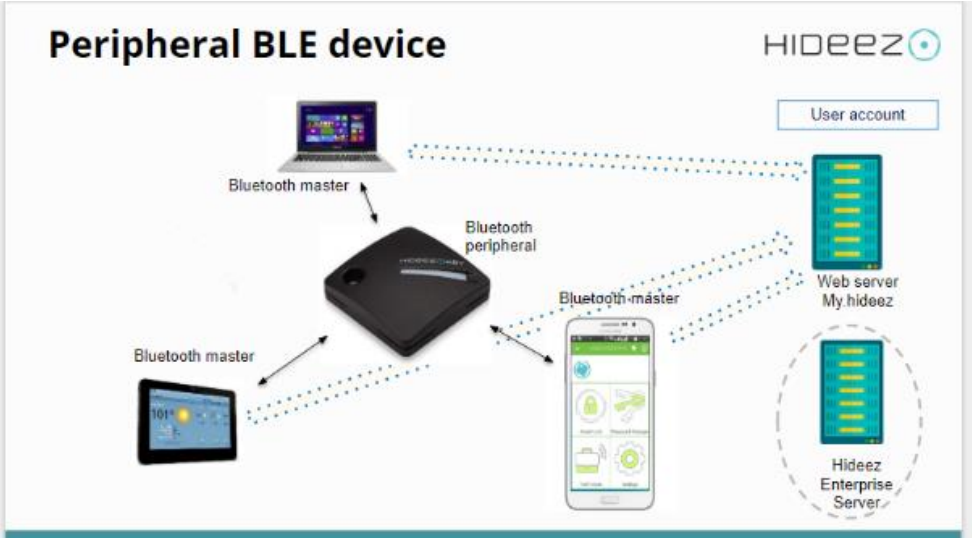
5) Segmentation
   Type: Comprises of one key password, public key infrastructure and others.
   Model: Comprises of smart card with pin, smart card with biometric technology, biometric technology with pin, two-factor biometric technology, one-time password with pin and others.
   Technology: Comprises of physical and logical access control, SafeNet OTP authenticators, out-of-band authenticators, Mobile PKI office suite, PKI authenticators and others.
   End User: Comprises of banking and finance, consumer electronics, healthcare, government, travel and immigration, military and defense, commercial security and others.

Regions: Comprises Geographical regions – North America, Europe, Asia Pacific and Rest of the World.

6) Competitor vulnerabilities

Standalone OTP	Real-time replay and social engineering attacks
Server storage of tokens	Seed leakage
USB Password Managers	Key in a keyhole. And hardware vulnerabilities: USB keyboard, virus transfer, Juice-jacking attacks
Telecom	Sim-swapping

7) How it works?



8) Hideez Key Technology
   - Authentication
   - Security
   - Auditability and accountability
   - Ease of Use: Efficiency and Productivity
   - Manageability

9) What is Hideez Password Manager?
   - Protects against digital identity theft, phishing,
   - credential stuffing, and account Take-overs
   - One Key for many services
   - Increased productivity of employees
   - Reduced cost of operations
   - Compatible with existing infrastructure
   - Decreased Annual Loss
   - Minimized risk of Human Error
   - Business continuity

10) What is Key Technology?

- Bluetooth 5.0 Low Energy (BLE) device. (Wireless digital access key and identity token)
- 2FA (TOTP) One-time passwords generator according RFC 6238
- Secure storage (156 kB) for sensitive data (logins, passwords, keys etc.)
- Provides Encryption API (RSA, ECC, AES-128)

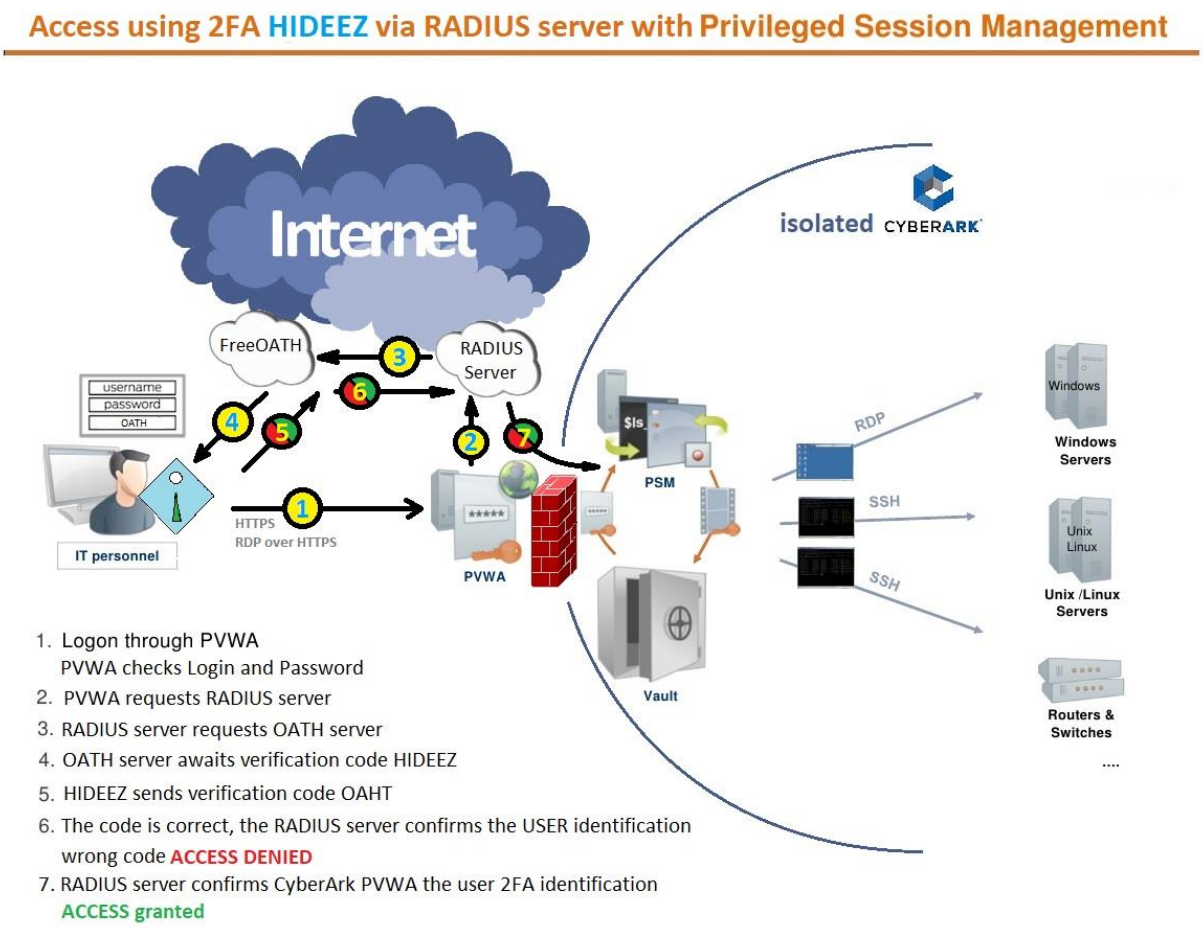
PRODUCT DIAGRAM & DESCRIPTION OF PRODUCT INTEGRATION

This solution sets us apart from other solutions, primarily due to the possibility of hardware storage of difficult-generated user passwords, a hard-to-select word format. Second, there is no need to have a telephone or other means of communication to confirm the user's identification in enterprises with high security requirements.

https://www.youtube.com/watch?v=13c1ExJswUA&

Example of setting up OTP generator for HideezKey for CyberArk Vault on 00 min 22 sec

Example of using Hideez Key to Login into CyberArk PVWA using OTP on 1 min 10 sec



PARTNER PRODUCT INSTALLATION & INTEGRATION CONFIGURATION

To deploy the HideezKey and CyberArk interaction scheme using the RADIUS security protocol, it is suggested to use any RADIUS authentication server (for example, FreeRADIUS https://github.com/FreeRADIUS/freeradius-server) installed using Ubuntu Server 18.04, with the settings of a secure channel using the CyberArk method, The Credential Provider and ASCP Implementation Guide, the Privileged Access Security Installation Guide, and the Privileged Access Security Implementation Guide. As well as bindings for the user authentication factor, the additionally raised system of multOTP authentication is https://github.com/multiOTP/multiOTPCredentialProvider or Google Authenticator https://github.com/google/google-authenticator-libpam . HideezKey acts as a wireless hardware password manager, as well as an access device to the user's workplace.

Instructions for setting up and using HideezKey (HideezSafe) are available at https://hideez.com/products/hideez-key or in the document repository https://hideez.com/pages/downloads.

INTEGRATION STEPS

Configuring CyberArk Privileged Security

Using the RADIUS authentication method

1. Log in to your Vault server and open a command prompt window. The command line utilities for configuring RADIUS are located in the Vault installation folder, usually in the directory C:\Program Files(x86)\PrivateArk\Server. Your Vault installation directory may vary.
2. Get the Vault certificate and private key from the certificate authority and install the Vault on your machine if it is not already present. CyberArk recommends that you do not use a self-signed certificate for RADIUS authentication.

If you do not already have a Vault certificate and private key, use the CACert.exe utility to generate a request.

This example command creates a certificate request file named VaultRadCert.req for the Vault vault.hideez.local DNS node with the IP address Vault 192.168.10.101 as the subject alternative name and additional identifying information about the organization requesting the certificate:

```
CACert request /reqoutfile c:\temp\VaultRadCert.req /country "US" /locality "Redwood City" /org "Hideez Inc" /orgunit "IT" /commonname "vault.hideez.local" /subjalt "IP:192.168.10.101"
```

Send this request to your certification authority to obtain a certificate for the Vault server. After you have a certificate, copy it to the Vault server and install it in the storage using the CACert utility.
In this command, an example of a certificate with a new name - cyberarkvault.cer:

```
CACert install /CertFileName c:\temp\cyberarkvault.cer
```

To read the full Vault certificate requirements and a detailed description of this step, see “Configuring RADIUS Authentication”, in the Privileged Access Security Installation Guide. For more information

about the CaCerArk Cert command and its parameters, see Appendix B, Privileged Access Security Installation Guide.
3. On the Vault server, launch the PrivateArk Server application and stop the Vault.
4. Create an encrypted file containing the same RADIUS secret using the CAVaultManager command
This example displays the secret radiussecret1 in the file radiusauth.dat.

CAVaultManager SecureSecretFiles /SecretType Radius /Secret radiussecret1 /SecuredFileName radiusauth.dat

ITADB399I Using encryption algorithms: Advanced Encryption Standard (AES), 256 bit,

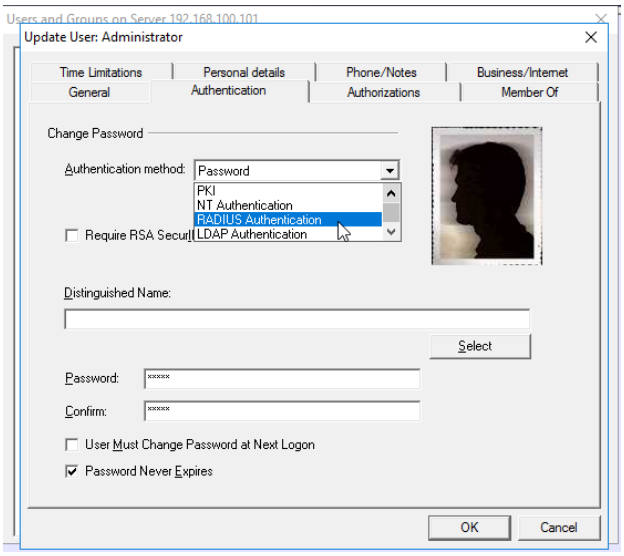
RSA (2048 bit), SHA2-512 (Protocol Integrity), SHA2-512 (Files Integrity).

5. Back up the DBParm.ini file in the Vault Server installation directory, and then open it in a text editor.
6. Add a new line RadiusServersInfo, which sets the IP address of your Rardius Server, the port, the host name of your Vault server and the name of the encrypted RADIUS secret file created using the CAVaultManager command in step 4.

RadiusServersInfo=192.168.10.99;1812;vault.hideez.local;radiusauth.dat

7. Return to the administration window of the PrivateArk Server and start the Vault server.
For more information and options, see the “Configuring RADIUS Authentication” section 2 through 5 in the Security Installation Guide for Preferred CyberArk Accounts.

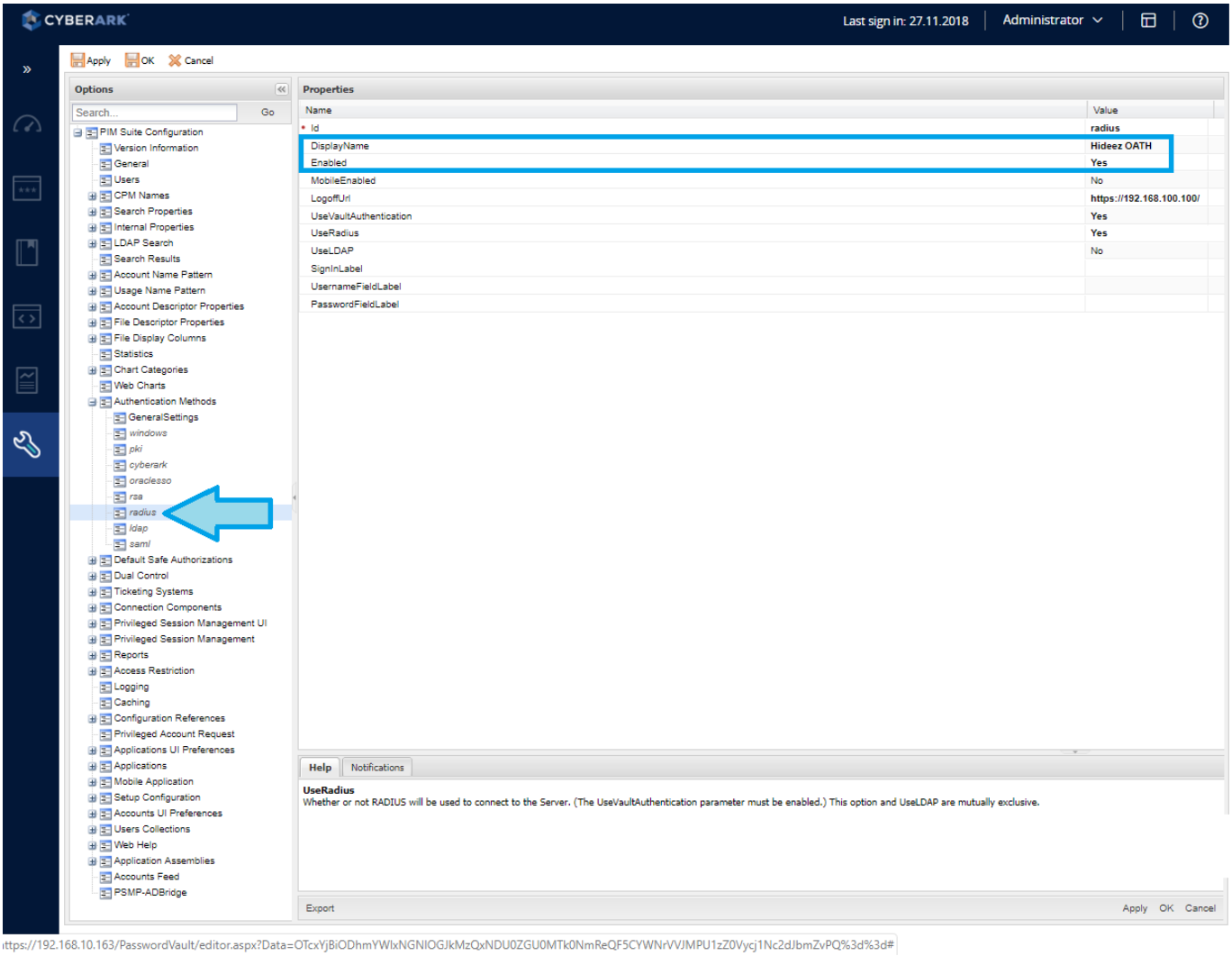
Configure user accounts for RADIUS
Update the authentication method for all users with whom you want to log in using HideezKey.
1. Launch the PrivateArk Client application. Double-click Server Storage to log in as the predefined Administrator user.
2. Perform Tools → Administrative Tools → Users and Groups.
3. Click on the user you want to switch to RADIUS authentication, and then click the Update button to display the user properties.
4. Go to the "Authentication" tab and select "RADIUS Authentication" in the "Authentication Method" drop-down list. Click "OK".



5. Exit the PrivateArk Client.

Setting up password access web access

1. Log in to Password Vault Web Access through your browser as a predefined Administrator user. This is usually done using https://yourvaultserver/PasswordVault or https://your.ip-adress.vault.server/PasswordVault
2. Click “ADMINISTRATION” at the top to go to the “System Configuration” page. Then click on the parameters in the Component Parameters table.
3. Scroll through the list of listed configuration items on the left to authentication methods. Expand this to display a list of tuning methods and click on the radius.
4. In the “Properties” table, enter a descriptive DisplayName, for example “HIDEEZ OATH”, and set “Enabled” to “Yes”.
5. Click "Apply" in the lower right corner, and then click "OK."

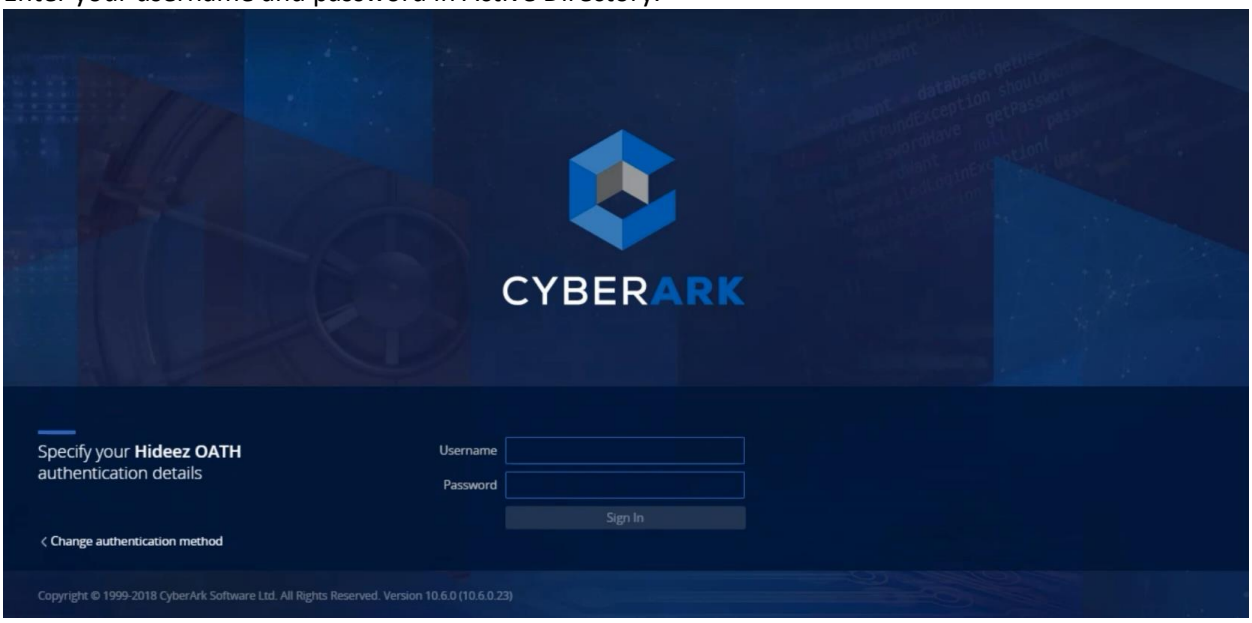


For more information about adding RADIUS authentication, see the “RADIUS Authentication” section in the Security Installation Guide for Preferred CyberArk Accounts.

Check setting

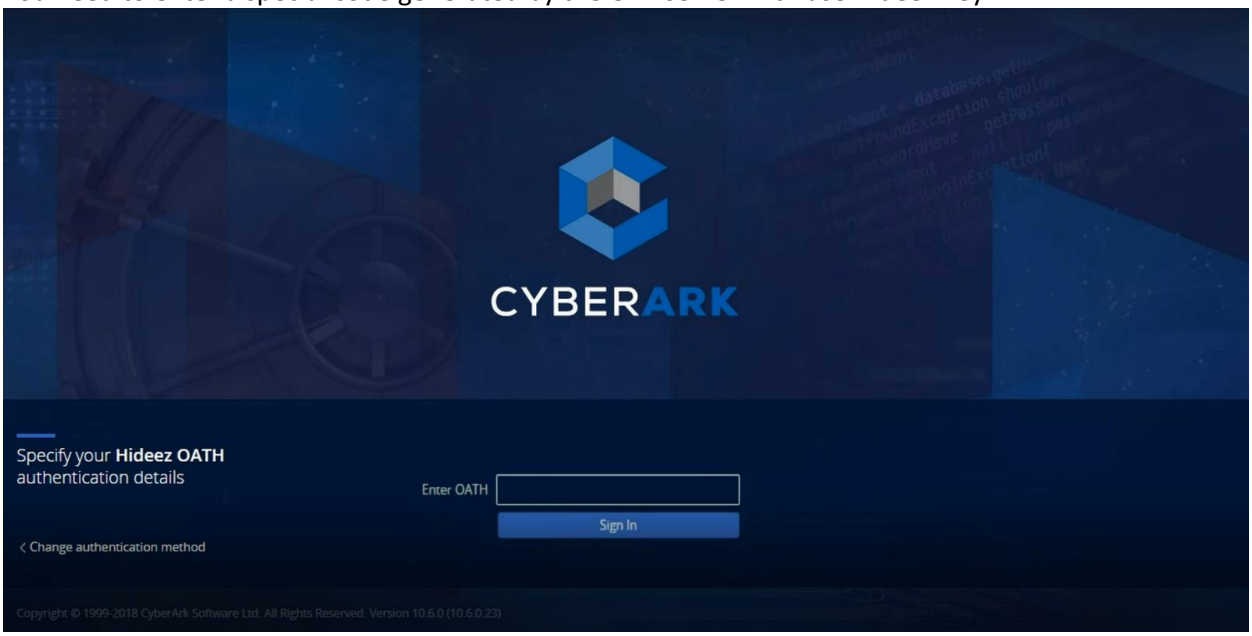
Go to the login page with privileged accounts and click on the new HIDEEZ OATH option (this name corresponds to the “DisplayName” you specified when configuring the RADIUS authentication method).

Enter your username and password in Active Directory.



After you have entered your username and password.

You need to enter a special code generated by the OTP server with use Hideez Key.



If the verification code matched, Access Granted.

PARTNER CONTACT INFO

Business Contact	Name	Oleg Naumenko
	Email	on@hideez.com
	Tel	+1 650 416 80 54
Business Contact	Name	Dmytro Gelgar
	Email	info@hideez.com
	Tel	+1 650 701 34 37
Technical Contact	Name	Andrii Bernatskyi
	Email	ab@hideez.com
	Tel	+1 650 762 63 22
Support Contact	Name	Denys Beztuzhev
	Email	support@hideez.com
	Tel	