

# Microsoft Direct Access Integration

## Contents

- 1 Introduction
- 2 Prerequisites
- 3 Baseline
- 4 Architecture
- 5 Installation
  - ◆ 5.1 PINsafe Configuration
    - ◇ 5.1.1 Configuring the RADIUS server
    - ◇ 5.1.2 Setting up the RADIUS NAS
    - ◇ 5.1.3 Enabling Session creation with username
  - ◆ 5.2 Microsoft Direct Access Integration
    - ◇ 5.2.1 Enable Two Factor Authentication
    - ◇ 5.2.2 Configure OTP Authentication Server
    - ◇ 5.2.3 CA Server Configuration
  - ◆ 5.3 Additional Installation Options
- 6 Verifying the Installation
- 7 Uninstalling the PINsafe Integration
- 8 Troubleshooting
- 9 Known Issues and Limitations
- 10 Additional Information

## Introduction

Microsoft Direct Access allows a VPN connection to be brought up when a user requires access to an organisations internal resources. PINsafe can authenticate a user accessing those internal resources using Dual channel authentication such as SMS, Mobile Phone Client and the Taskbar utility [Taskbar How to Guide](#) and [Token](#).

## Prerequisites

Microsoft Direct Access fully configured

Microsoft CA server for OTP authentication

PINsafe 3.x

## Baseline

Microsoft UAG SP1 with Direct access configured

PINsafe 3.8

## Architecture

When a Direct Access connection is made, a pop up appears for the user prompting them to enter their One Time Code. This is then checked by the UAG against PINsafe using RADIUS authentication.

## Installation

### PINsafe Configuration

#### Configuring the RADIUS server

Configure the RADIUS settings using the RADIUS configuration page in the PINsafe Administration console. In this example (see diagram below) the RADIUS Mode is set to ?Enabled? and the HOST IP (the PINsafe server) is set to 0.0.0.0. (leaving the field empty has the same result). This means that the server will answer all RADIUS requests received by the server regardless of the IP address that they were sent to.

Note: for appliances, the PINsafe VIP should not be used as the server IP address, see [VIP on PINsafe Appliances](#)

## RADIUS>Server

Please enter the details for the RADIUS server.

Server enabled:	<input type="text" value="Yes"/>
IP address:	<input type="text" value="0.0.0.0"/>
Authentication port:	<input type="text" value="1812"/>
Accounting port:	<input type="text" value="1813"/>
Maximum no. sessions:	<input type="text" value="50"/>
Permit empty attributes:	<input type="text" value="No"/>
Filter ID:	<input type="text" value="No"/>
Additional RADIUS logging:	<input type="text" value="Both"/>
Enable debug:	<input type="text" value="Yes"/>
Radius Groups:	<input type="text" value="Yes"/>
Radius Group Keyword:	<input type="text" value="POLICY"/>

### Setting up the RADIUS NAS

Set up the NAS using the Network Access Servers page in the PINsafe Administration console. Enter a name for the VPN server. The IP address has been set to the IP of the VPN appliance, and the secret ?secret? assigned that will be used on both the PINsafe server and VPN RADIUS configuration.

## RADIUS>NAS

Please enter the details for any RADIUS network access servers. A NAS is permitted to access the authentication server via the RADIUS interface.

NAS Identifier:	<input type="text" value="Device Name"/>
Hostname/IP:	<input type="text" value="192.168.0.1"/>
Secret:	<input type="password" value="••••••"/>
EAP protocol:	<input type="text" value="None"/>
Group:	<input type="text" value="---ANY---"/>
Authentication Mode:	<input type="text" value="All"/>
Change PIN warning:	<input type="text" value="No"/>
<input type="button" value="Apply"/> <input type="button" value="Reset"/>	

You can specify an EAP protocol if required, others CHAP, PAP and MSCHAP will be supported. All users will be able to authenticate via this NAS unless to restrict authentication to a specific repository group.

### Enabling Session creation with username

PINsafe can be configured to use the Taskbar to present a Turing image to users when prompted for authentication by Direct Access. See [Taskbar How to Guide](#)

To allow Single Channel authentication on PINsafe follow the below steps.

Go to the ?Single Channel? Admin page and set ?Allow Session creation with Username:? to YES.

To test your configuration you can use the following URL using a valid PINsafe username:

Appliance

[https://PINsafe\\_server\\_IP:8443/proxy/SCImage?username=testuser](https://PINsafe_server_IP:8443/proxy/SCImage?username=testuser)

For a software only install see [Software Only Installation](#)

### Microsoft Direct Access Integration

Ensure that the Microsoft Direct Access is fully working and tested before starting the PINsafe integration.

### Enable Two Factor Authentication

On the Forefront UAG Direct Access configuration page select under Step 2 Optional Settings the link for *Two-Factor Authentication*

**Microsoft Forefront Unified Access Gateway Management**

File View Admin Messages Help

Forefront UAG

- HTTP Connections
- HTTPS Connections
- DirectAccess

Microsoft Forefront Unified Access Gateway 2010

DirectAccess configuration last activated: Thursday, March 08, 2012 2:13:11 PM

Read the UAG DirectAccess [deployment](#) and [planning](#) guides

**Step 1**

 **Clients and GPOs**  
[Learn more](#)

Select the groups of clients allowed to connect using DirectAccess.

[Edit](#)

Optional Settings:  
[Client Connectivity Assistant \(On\)](#)

**Internet**

**Step 2**

 **DirectAccess Server**  
[Learn more](#)

Configure connectivity and security policies for the UAG DirectAccess Server.

[Edit](#)

Optional Settings:  
[Two-Factor Authentication](#)  
[Network Access Protection](#)  
[Force Tunneling](#)  
[Server Groups](#)

Click Apply Policy to apply the configuration, or click Export to save the configuration, and apply it with PowerShell. Click Activate after applying the configuration.

Message Time	Message Type	Message

Click on *Require two-factor authentication*

## Two-Factor Authentication Configuration

### Client Authentication

You can require clients to use two-factor authentication. Select the method used by UAG DirectAccess for two-factor authentication.

- Require two-factor authentication
  - Clients will log on using a PKI smart card
  - Clients will authenticate using a one-time password (OTP)

[Learn more...](#)

< Back

Next >

Finish

Click on *Clients will authenticate using a one-time password (OTP)*

## Two-Factor Authentication Configuration

### Client Authentication

OTP Authentication

OTP CA Servers

OTP CA Templates

You can require clients to use two-factor authentication. Select the method used by UAG DirectAccess for two-factor authentication.

- Require two-factor authentication
  - Clients will log on using a PKI smart card
  - Clients will authenticate using a one-time password (OTP)

[Learn more...](#)

< Back

Next >

Finish

### Configure OTP Authentication Server

On the OTP Authentication tab click Add

## Two-Factor Authentication Configuration

Client Authentication

**OTP Authentication**

OTP CA Servers

OTP CA Templates

DirectAccess client authentication is configured to use OTP. Select the OTP authentication server.

OTP authentication server:



The OTP authentication servers can be edited and deleted in the Authentication and Authorization Servers dialog box, available in the Admin menu.



Require OTP user names to match Active Directory user names  
With this setting enabled, users log on in UPN format (username@domain).

[Learn more...](#)

&lt; Back

Next &gt;

Finish

Select Server Type RADIUS and enter the following information:

- Server Name: A descriptive name for the RADIUS server
- Port: RADIUS port used by the Swivel server, usually 1812
- IP address/host: The Swivel RADIUS server
- Alternate IP/host: A secondary Swivel RADIUS server
- Alternate port: The port used by the secondary Swivel server, usually 1812
- Secret Key: A shared secret entered on the Swivel servers.

**Add Authentication Server**

Server type:

Server name:

---

IP address/host:

Port:

Alternate IP/host:

Alternate port:

Secret key:

Ensure that the new Swivel server is selected. Optionally select *Require OTP user names to match Active Directory user names with this setting enabled*, users log on in UPN format (*username@domain*), then the user name will be automatically populated at the direct access login.

**UAG DirectAccess Server Configuration**

## Two-Factor Authentication Configuration

Client Authentication

**OTP Authentication**

OTP CA Servers

OTP CA Templates

DirectAccess client authentication is configured to use OTP. Select the OTP authentication server.

OTP authentication server:

 The OTP authentication servers can be edited and deleted in the Authentication and Authorization Servers dialog box, available in the Admin menu.

Require OTP user names to match Active Directory user names  
With this setting enabled, users log on in UPN format (*username@domain*).

[Learn more...](#)

## CA Server Configuration

Under OTP CA Servers click on Add and select the OTP CA Server.

The screenshot shows the 'UAG DirectAccess Server Configuration' wizard, specifically the 'Two-Factor Authentication Configuration' step. The left-hand navigation pane includes 'Client Authentication', 'OTP Authentication', 'OTP CA Servers' (which is selected and highlighted in blue), and 'OTP CA Templates'. The main content area contains the following text: 'UAG DirectAccess uses certificates for OTP authentication. Select the CA servers that will issue certificates and specify how CA templates are configured and deployed.' Below this is a sub-instruction: 'Specify the OTP CA servers. Add them in the order they should be queried during OTP authentication.' This is followed by a large empty rectangular box for listing servers, with 'Add' and 'Remove' buttons on the right side. Underneath the box is a text input field labeled 'Common parent CA to which the OTP CA servers chain:'. Below that is the section 'Select how CA templates are deployed:' with two radio button options: 'Use a UAG DirectAccess script to configure CA templates and automatic renewal' (which is selected) and 'Use existing CA templates located on the CA servers, and configure automatic renewal manually'. At the bottom of the main area is an information icon and a note: 'When you create the script on the next page of the wizard, you can apply it immediately, or you can save the script and apply it at a later time. When you apply the script, all existing CA templates are replaced on the CA servers.' The bottom of the wizard features a 'Learn more...' link on the left and '< Back', 'Next >', and 'Finish' buttons on the right.

This example is configured to use existing CA templates.

# Two-Factor Authentication Configuration

Client Authentication

OTP Authentication

OTP CA Servers

OTP CA Templates

UAG DirectAccess uses certificates for OTP authentication. Select the CA servers that will issue certificates and specify how CA templates are configured and deployed.

Specify the OTP CA servers. Add them in the order they should be queried during OTP authentication.

SVVCERT	Remove
	Up
	Down

Common parent CA to which the OTP CA servers chain:

SVVCERT

Select how CA templates are deployed:

- Use a UAG DirectAccess script to configure CA templates and automatic renewal
- Use existing CA templates located on the CA servers, and configure automatic renewal manually



If you use existing CA templates, configure them manually on the CA servers, and select the appropriate page of the wizard.

[Learn more...](#)

< Back

Next >

Finish

Select the required templates

## Two-Factor Authentication Configuration

Client Authentication

OTP Authentication

OTP CA Servers

OTP CA Templates

Select the CA template used for issuing certificates for OTP client authentication and identifying the UAG DirectAccess server to OTP clients. Specify a certificate renewal policy.

OTP certificate template for client authentication:

OTPUser

OTP certificate template for workstation authentication:

OTPWorkstation

Enable certificate renewal. Maximum renewal period (days): 7



When you select this option, you have to configure the selected templates on the CA server for OTP authentication. They will not be configured automatically by UAG DirectAccess.

Click to verify that the CA servers can be used for OTP authentication:

Validate



Certificate OTPUser cannot be enrolled. Ensure that each UAG DirectAccess server has Enroll permissions on the certificate template.

[Learn more...](#)

< Back

Next >

Finish

Validate the CA templates

## Two-Factor Authentication Configuration

Client Authentication

OTP Authentication

OTP CA Servers

OTP CA Templates

Select the CA template used for issuing certificates for OTP client authentication and identifying the UAG DirectAccess server to OTP clients. Specify a certificate renewal policy.

OTP certificate template for client authentication:

OTPUser

OTP certificate template for workstation authentication:

OTPWorkstation

Enable certificate renewal. Maximum renewal period (days): 7



When you select this option, you have to configure the selected templates on the CA server for OTP authentication. They will not be configured automatically by UAG DirectAccess.

Click to verify that the CA servers can be used for OTP authentication:

Validate



Validation successful. CA servers are configured correctly.

[Learn more...](#)

< Back

Next >

Finish

### Additional Installation Options

### Verifying the Installation

Access with the Direct Access client entering username, AD password and One Time Code. If the option to *Require OTP user names to match Active Directory user names* then the user name will be automatically populated.

Check the UAG and PINsafe logs for authentication messages.

### Uninstalling the PINsafe Integration

### Troubleshooting

### Known Issues and Limitations

### Additional Information

Microsoft DirectAccess