SafeNet Authentication Client

Integration Guide

Using SAC CBA for Microsoft DirectAccess

THE
DATA
PROTECTION
COMPANY

Document Information

Document Part Number	007-012960-001, Rev. A
Release Date	April 2015

Trademarks

All intellectual property is protected by copyright. All trademarks and product names used or referred to are the copyright of their respective owners. No part of this document may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, chemical, photocopy, recording, or otherwise, without the prior written permission of SafeNet, Inc.

Disclaimer

SafeNet makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, SafeNet reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon SafeNet to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

SafeNet invites constructive comments on the contents of this document. These comments, together with your personal and/or company details, should be sent to the address or email below.

Contact Method	Contact Information
Mail	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017, USA
Email	TechPubs@safenet-inc.com

Contents

Third-Party Software Acknowledgement

This document is intended to help users of SafeNet products when working with third-party software, such as Microsoft DirectAccess.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users – often remote users – requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

PKI is and effective strong authentication solution to the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. SafeNet’s certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SafeNet Authentication Client (SAC). The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization's authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet’s hardware or software tokens devices. SAM is designed and developed based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets different organizations’ PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the *SafeNet Authentication Manager Administrator Guide*.

DirectAccess is a VPN-like technology that provides intranet connectivity to client computers when they are connected to the Internet. Unlike many traditional VPN connections that must be initiated and terminated by explicit user action, DirectAccess connections connect automatically, as soon as the computer connects to the Internet. DirectAccess was introduced in Windows Server 2008 R2, and requires clients running either the Windows 7 or Windows 8 Enterprise edition.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Microsoft DirectAccess using SafeNet tokens.

It is assumed that the Microsoft DirectAccess environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Microsoft DirectAccess can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet products.

Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC)** — SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **Microsoft DirectAccess**

Environment

The integration environment that was used in this document is based on the following software versions:

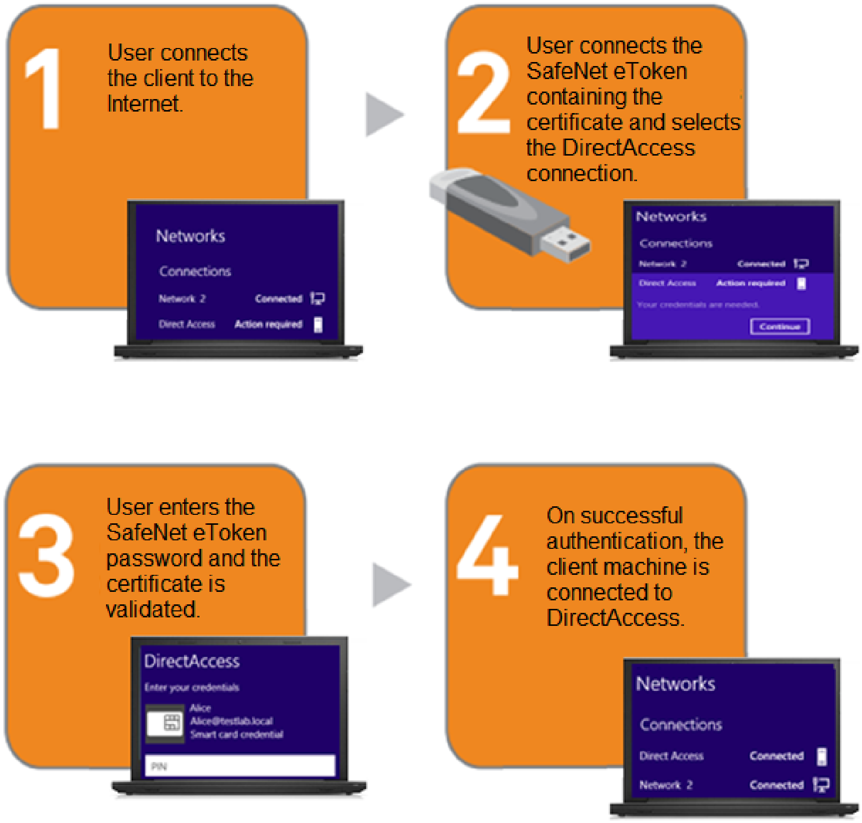
- **SafeNet Authentication Client (SAC)**—Version 9.0
- **Microsoft DirectAccess**—Windows Server 2012 R2

Audience

This document is targeted to system administrators who are familiar with Microsoft DirectAccess and are interested in adding certificate-based authentication capabilities using SafeNet tokens.

CBA Flow using SAC

The diagram below illustrates the flow of certificate-based authentication:


1
User connects the client to the Internet.
Networks
Connections
Network 2 Connected
Direct Access Action required
2
User connects the SafeNet eToken containing the certificate and selects the DirectAccess connection.
Networks
Connections
Network 2 Connected
Direct Access Action required
Your credentials are needed.
Continue
3
User enters the SafeNet eToken password and the certificate is validated.
DirectAccess
Enter your credentials
Alice
Alice@testlab.local
Smart card credential
PIN
4
On successful authentication, the client machine is connected to DirectAccess.
Networks
Connections
Direct Access Connected
Network 2 Connected

1. User connects the client to the Internet and tries to connect to the DirectAccess Server.
2. User connects the SafeNet eToken containing the certificate physically into USB port of machine, and then selects the DirectAccess connection.
3. User enters the SafeNet eToken password, and the certificate is validated.
4. On successful authentication, the client machine is connected to DirectAccess.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for Microsoft DirectAccess using SafeNet tokens:

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- If SAM is used to manage the tokens, TPO should be configured with MS CA Connector. For further details, refer to the section “Connector for Microsoft CA” in the *SafeNet Authentication Manager Administrator’s Guide*.
- Users must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client (9.0) should be installed on all client machines.

Supported Tokens in SAC

SAC supports a number of tokens that can be used as second authentication factor for users who authenticate to Microsoft DirectAccess.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

Certificate-based USB tokens

- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

Smart Cards

- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

Certificate-based Hybrid USB Tokens

- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)

Software Tokens

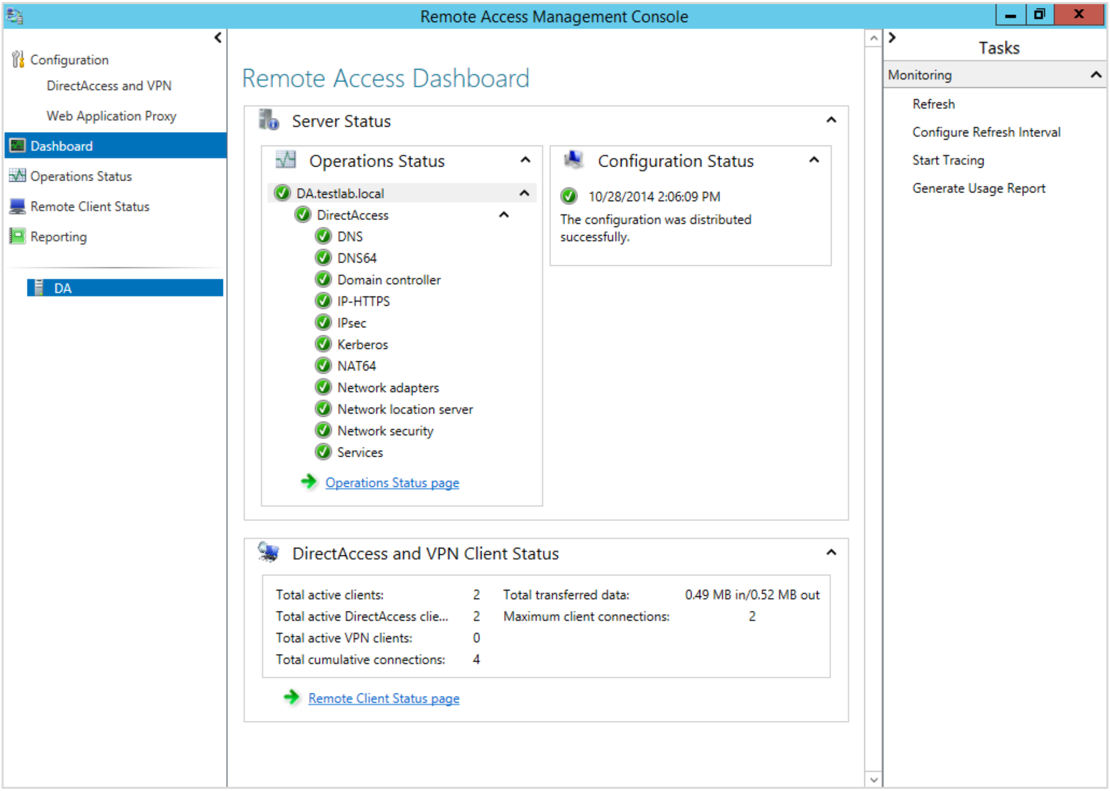
- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring Microsoft DirectAccess

Complete the procedures in this section to configure DirectAccess for two-factor authentication so users can authenticate using certificates on their eTokens.

Configuring the DirectAccess Server

1. Open the Remote Access Management Console.



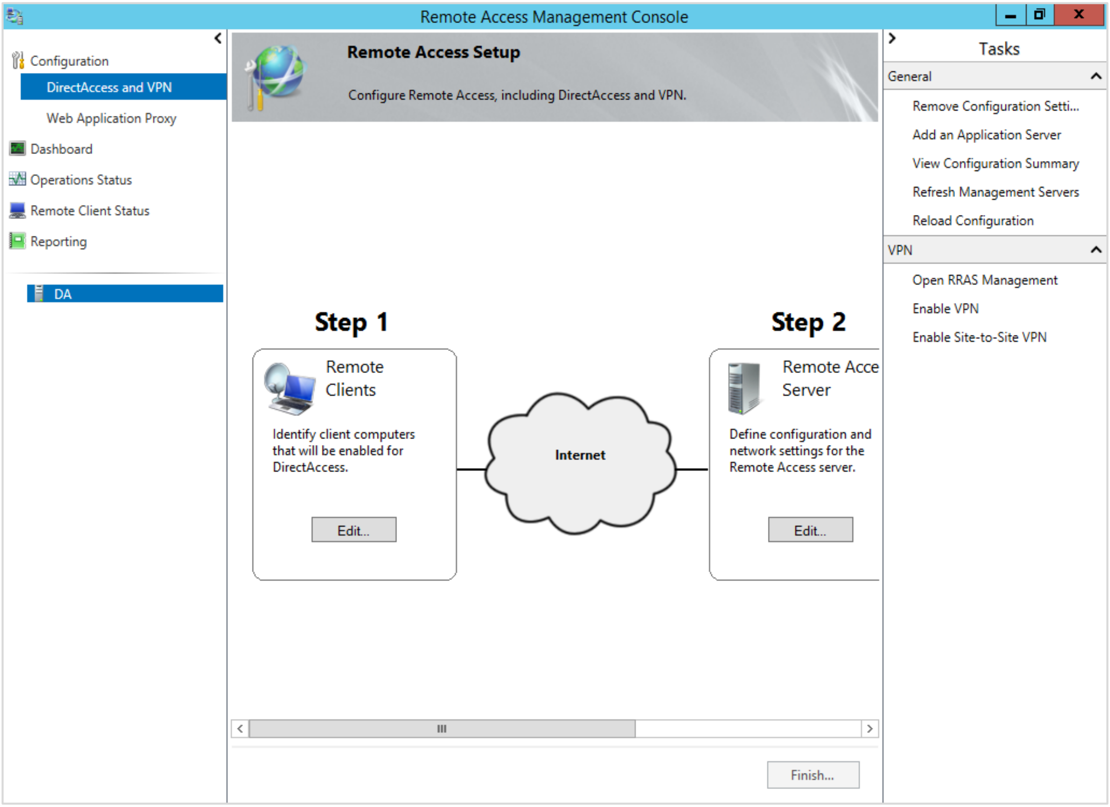
DA.testlab.local
DirectAccess
DNS
DNS64
Domain controller
IP-HTTPS
IPsec
Kerberos
NAT64
Network adapters
Network location server
Network security
Services

10/28/2014 2:06:09 PM
The configuration was distributed successfully.

Total active clients:	2	Total transferred data:	0.49 MB in/0.52 MB out
Total active DirectAccess clie...	2	Maximum client connections:	2
Total active VPN clients:	0		
Total cumulative connections:	4		

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

2. Under **Configuration**, select **DirectAccess and VPN**, and then under **Step 2**, click **Edit**.



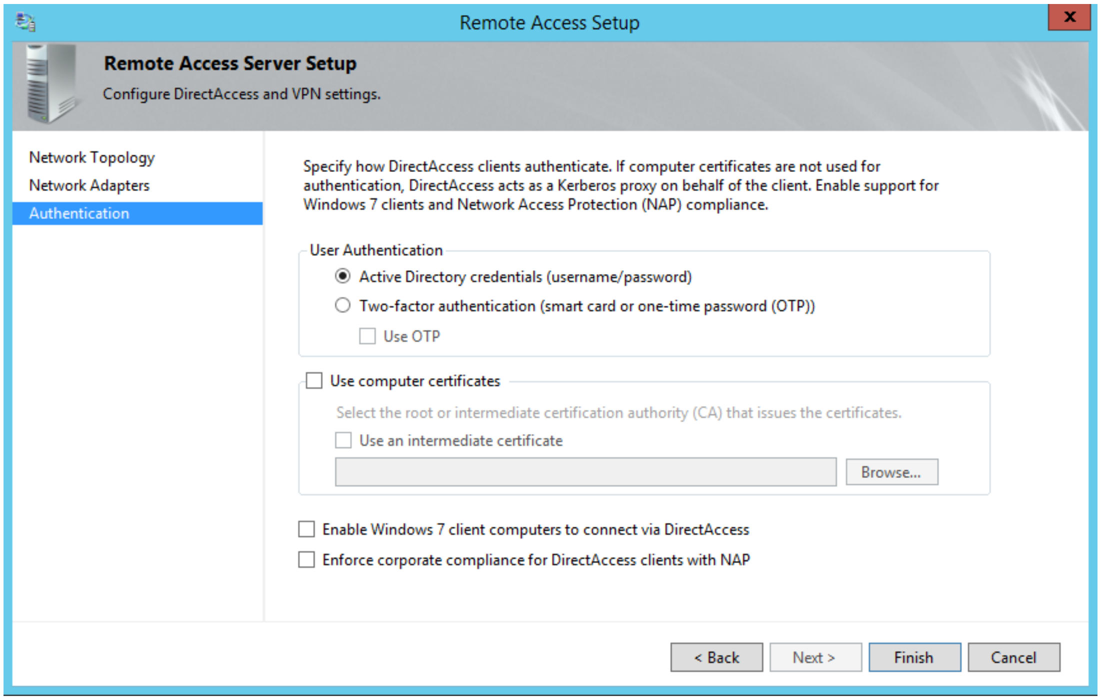
Configure Remote Access, including DirectAccess and VPN.

Identify client computers that will be enabled for DirectAccess.

Define configuration and network settings for the Remote Access server.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

3. Select **Authentication**.



Configure DirectAccess and VPN settings.

Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.

User Authentication

● Active Directory credentials (username/password)

○ Two-factor authentication (smart card or one-time password (OTP))

□ Use OTP

□ Use computer certificates

Select the root or intermediate certification authority (CA) that issues the certificates.

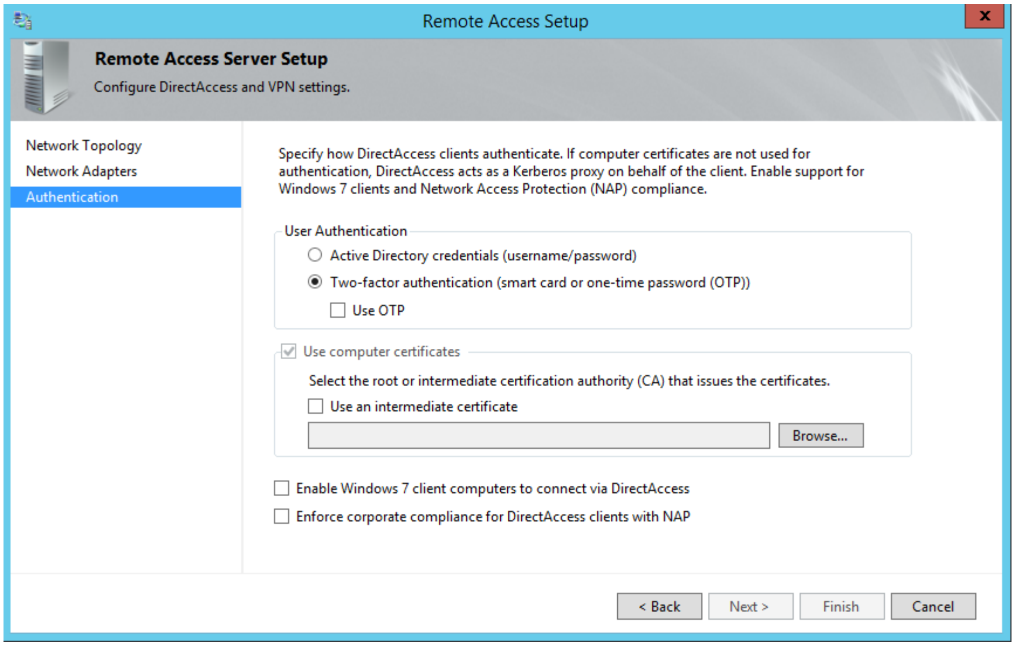
□ Use an intermediate certificate

□ Enable Windows 7 client computers to connect via DirectAccess

□ Enforce corporate compliance for DirectAccess clients with NAP

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

4. Under **User Authentication**, select **Two-factor authentication (smart card or one-time password (OTP))**. Make sure the **Use OTP** check box is not selected.



Remote Access Setup

Remote Access Server Setup

Configure DirectAccess and VPN settings.

Network Topology
Network Adapters
Authentication

Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.

User Authentication

○ Active Directory credentials (username/password)

● Two-factor authentication (smart card or one-time password (OTP))

□ Use OTP

☑ Use computer certificates

Select the root or intermediate certification authority (CA) that issues the certificates.

□ Use an intermediate certificate

Browse...

□ Enable Windows 7 client computers to connect via DirectAccess

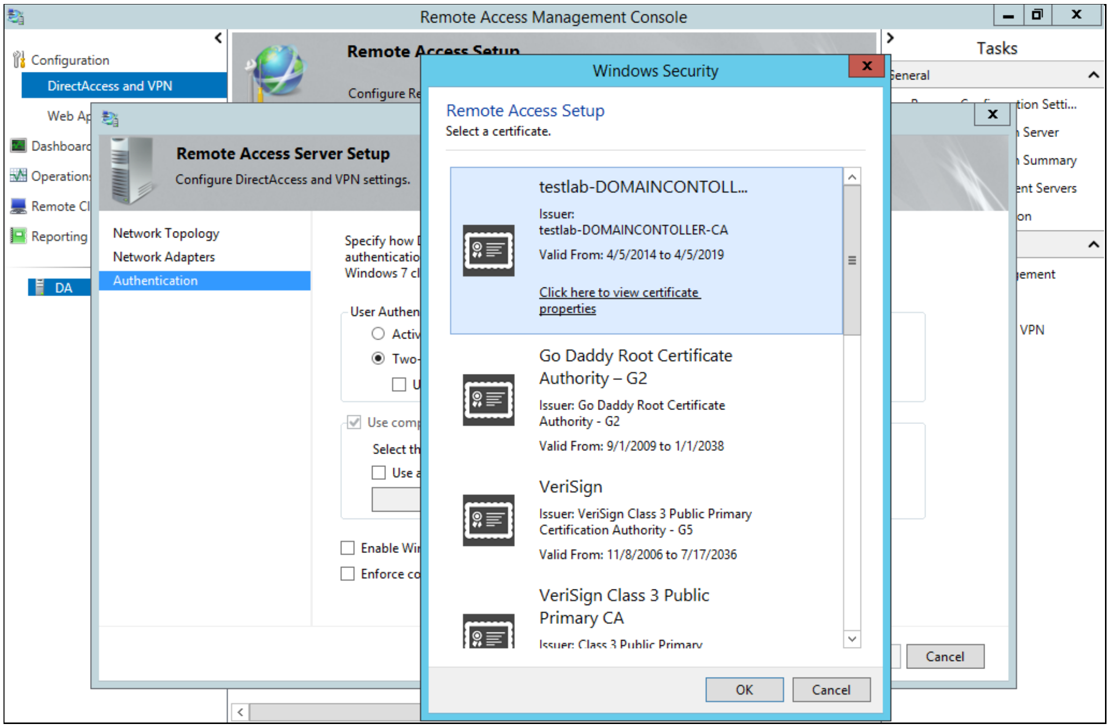
□ Enforce corporate compliance for DirectAccess clients with NAP

< Back | Next > | Finish | Cancel

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

5. Under **Use computer certificates**, click **Browse**.

6. On the **Windows Security** window, select the root or intermediate certification authority (CA) certificate that issues the certificates, and then click **OK**.



Windows Security

Remote Access Setup

Select a certificate.

testlab-DOMAINCONTOLL...
Issuer:
testlab-DOMAINCONTOLLER-CA
Valid From: 4/5/2014 to 4/5/2019
Click here to view certificate properties

Go Daddy Root Certificate Authority – G2
Issuer: Go Daddy Root Certificate Authority - G2
Valid From: 9/1/2009 to 1/1/2038

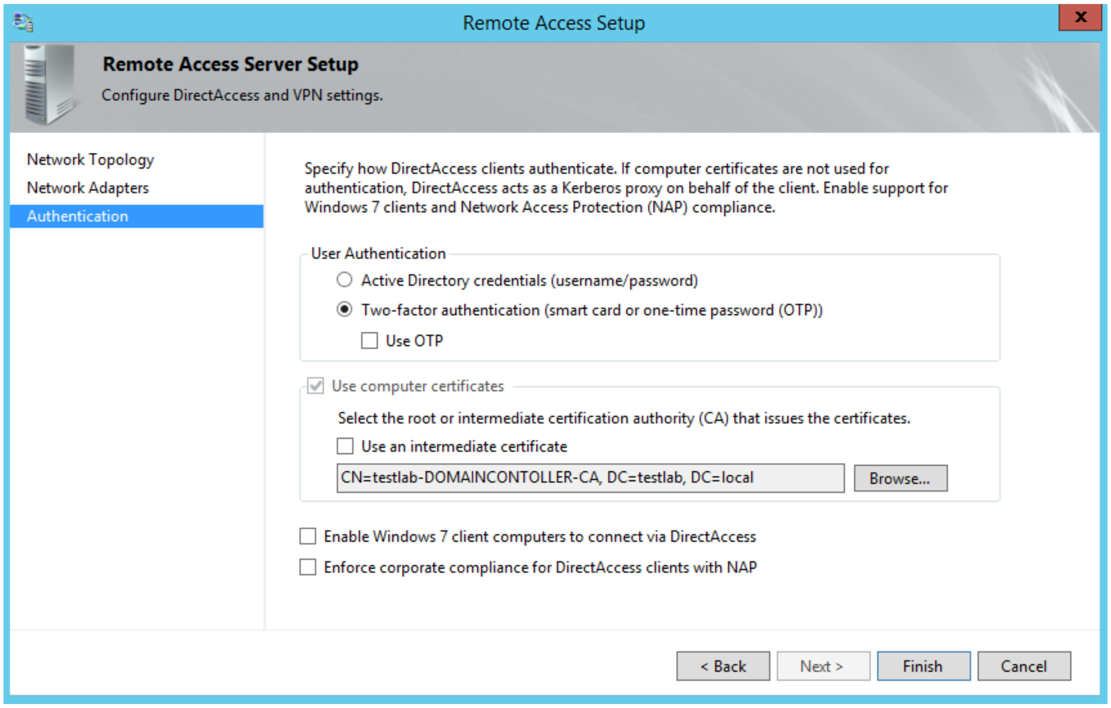
VeriSign
Issuer: VeriSign Class 3 Public Primary Certification Authority - G5
Valid From: 11/8/2006 to 7/17/2036

VeriSign Class 3 Public Primary CA
Issuer: Class 3 Public Primary

OK | Cancel

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

7. On the **Remote Access Setup** window, click **Finish**.



Remote Access Setup

Remote Access Server Setup

Configure DirectAccess and VPN settings.

Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess acts as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.

User Authentication

○ Active Directory credentials (username/password)

● Two-factor authentication (smart card or one-time password (OTP))

□ Use OTP

☑ Use computer certificates

Select the root or intermediate certification authority (CA) that issues the certificates.

□ Use an intermediate certificate

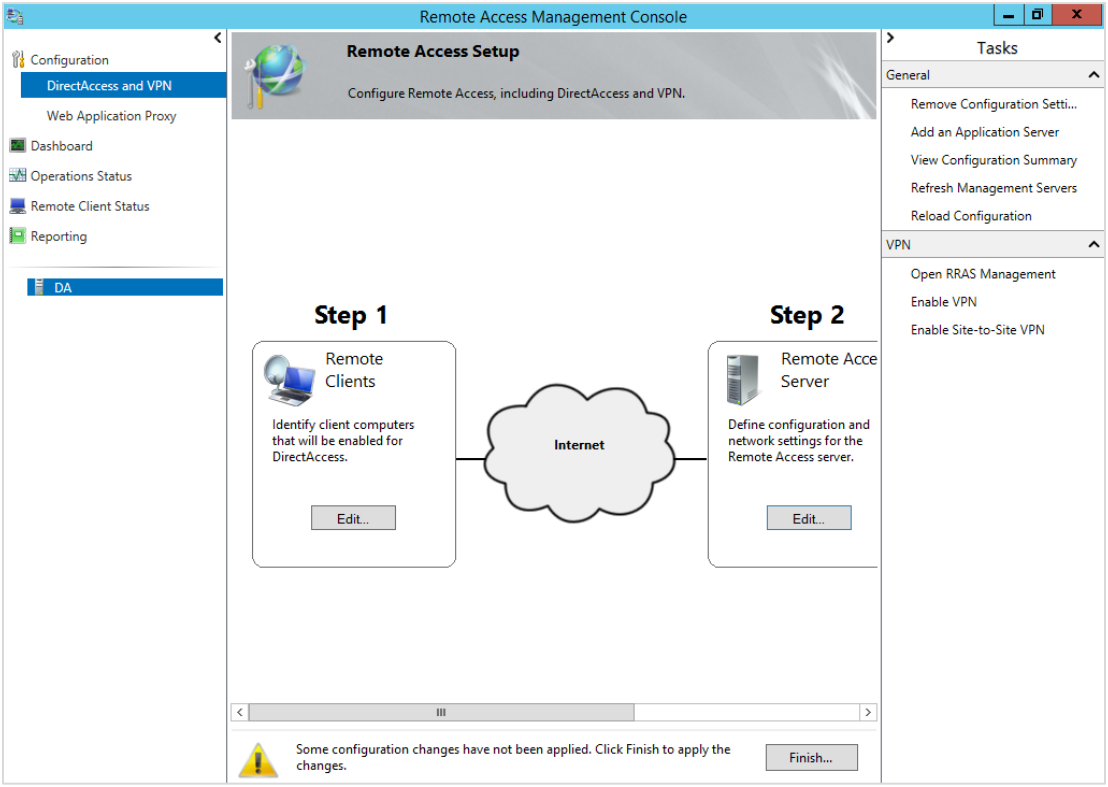
CN=testlab-DOMAINCONTOLLER-CA, DC=testlab, DC=local

□ Enable Windows 7 client computers to connect via DirectAccess

□ Enforce corporate compliance for DirectAccess clients with NAP

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

8. Click **Finish** again.



Remote Access Management Console

Remote Access Setup

Configure Remote Access, including DirectAccess and VPN.

Step 1

Remote Clients

Identify client computers that will be enabled for DirectAccess.

Step 2

Remote Acce Server

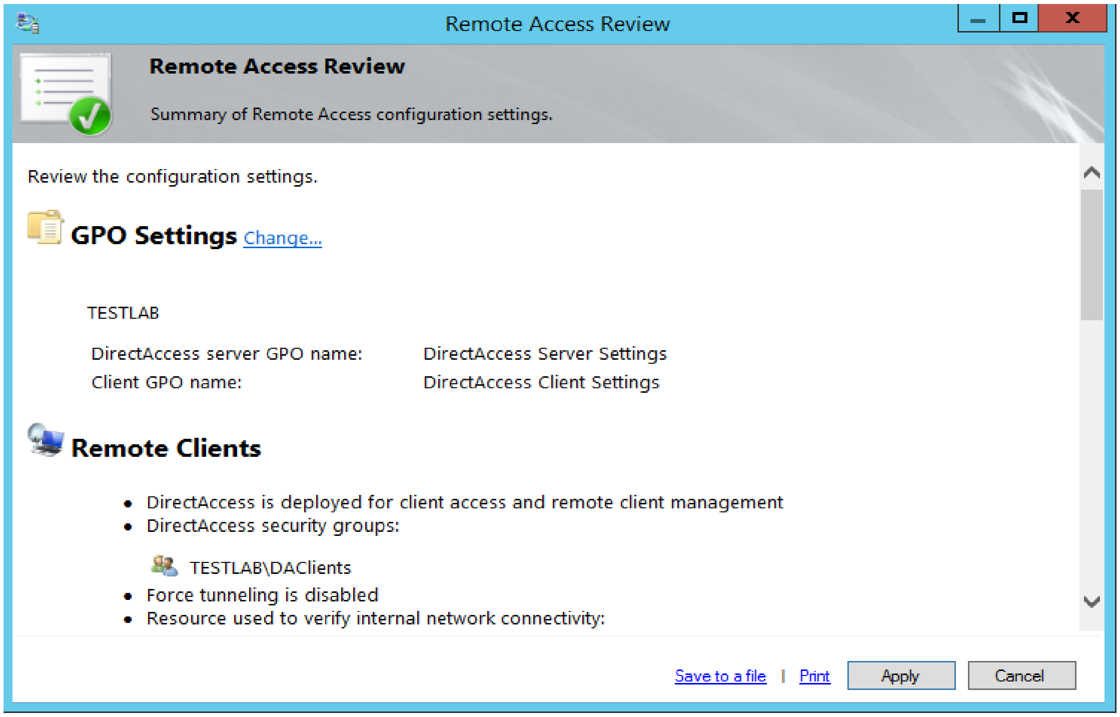
Define configuration and network settings for the Remote Access server.

Edit...
Tasks
General
Remove Configuration Setti...
Add an Application Server
View Configuration Summary
Refresh Management Servers
Reload Configuration
VPN
Open RRAS Management
Enable VPN
Enable Site-to-Site VPN

Some configuration changes have not been applied. Click Finish to apply the changes.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

9. On the **Remote Access Review** window, review the settings, and then click **Apply**.



Remote Access Review

Summary of Remote Access configuration settings.

Review the configuration settings.

GPO Settings Change...

TESTLAB

DirectAccess server GPO name: DirectAccess Server Settings
Client GPO name: DirectAccess Client Settings

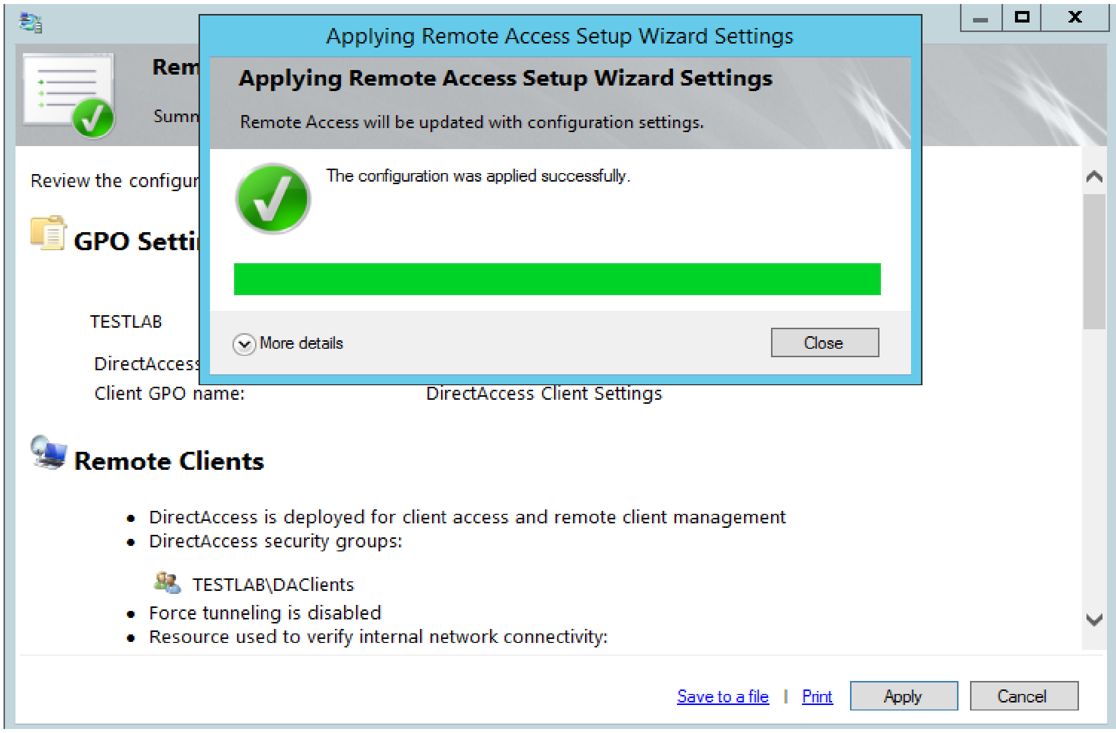
Remote Clients

- DirectAccess is deployed for client access and remote client management
- DirectAccess security groups:

  TESTLAB\DAClients
- Force tunneling is disabled
- Resource used to verify internal network connectivity:

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

10. On the **Applying Remote Access Setup Wizard Settings** window, click **Close**.



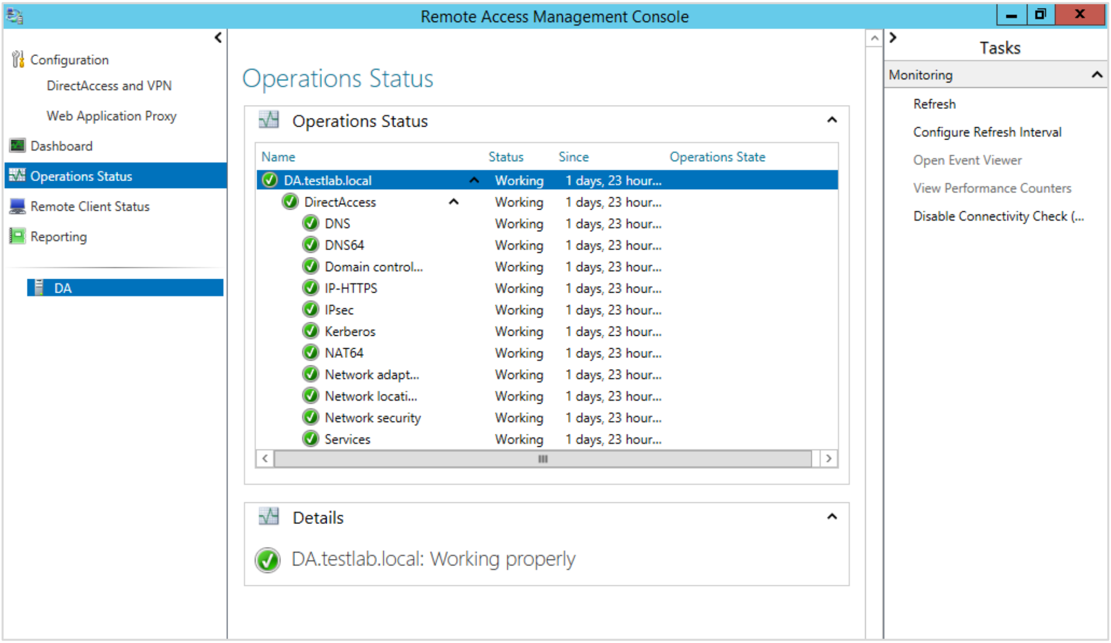
Applying Remote Access Setup Wizard Settings

Remote Access will be updated with configuration settings.

The configuration was applied successfully.

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

11. Select **Operations Status**. Verify that the status for each configuration is **Working**.



Name	Status	Since	Operations State
DA.testlab.local	Working	1 days, 23 hour...	
DirectAccess	Working	1 days, 23 hour...	
DNS	Working	1 days, 23 hour...	
DNS64	Working	1 days, 23 hour...	
Domain control...	Working	1 days, 23 hour...	
IP-HTTPS	Working	1 days, 23 hour...	
IPsec	Working	1 days, 23 hour...	
Kerberos	Working	1 days, 23 hour...	
NAT64	Working	1 days, 23 hour...	
Network adapt...	Working	1 days, 23 hour...	
Network locati...	Working	1 days, 23 hour...	
Network security	Working	1 days, 23 hour...	
Services	Working	1 days, 23 hour...	

DA.testlab.local: Working properly

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

12. Close the Remote Access Management Console.

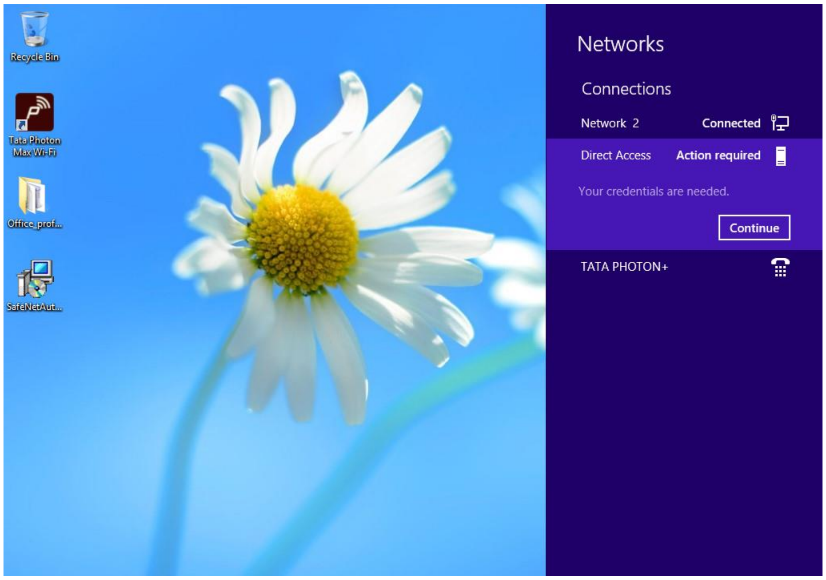
Configuring the DirectAccess Client

1. Connect the client to the corporate network.
2. Open **Windows PowerShell** as an **Administrator**.
3. Type **Get-DnsClientNrptPolicy**, and the press **Enter**. The Name Resolution Policy Table (NRPT) entries for DirectAccess are displayed.
4. Type **Get-NCSIPolicyConfiguration**, and then press **Enter**. The Network Connectivity Status Indicator (NCSI) settings deployed by the DirectAccess Getting Started Wizard are displayed.
5. Type **gpupdate /force**, and then press **Enter**.

Running the Solution

Check the final running solution of DirectAccess with SafeNet Authentication Client. Before proceeding, make sure that SafeNet Authentication client is installed on the client machine.

1. Connect the client to the Internet.
2. Connect the SafeNet eToken physically into a USB slot of the machine.
3. Click the network icon in the notification area (system tray).
4. Click the Direct Access connection name, and then click **Continue**.



Networks

Connections

Network 2 — Connected

Direct Access — Action required

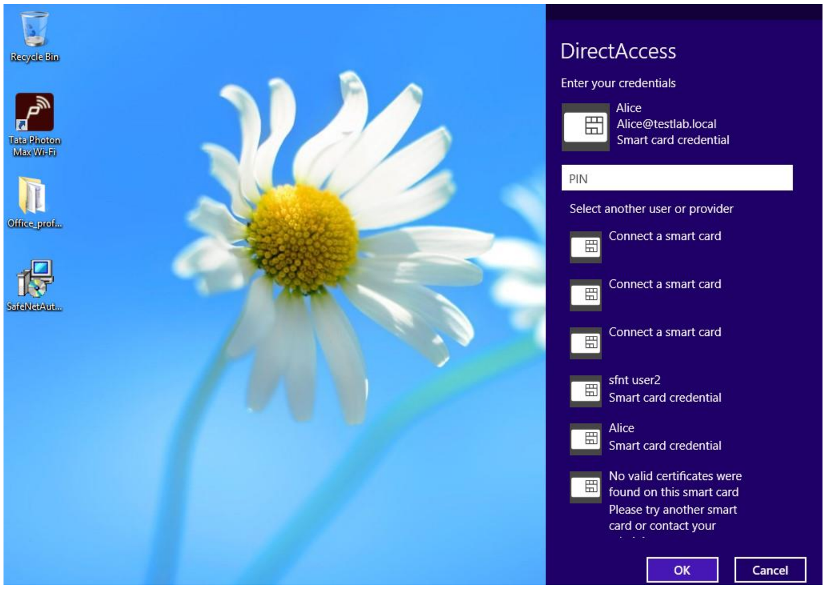
Your credentials are needed.

Continue

TATA PHOTON+

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

5. Select the appropriate user certificate, enter the token password in **PIN** field, and then click **OK**.



DirectAccess

Enter your credentials

Alice
Alice@testlab.local
Smart card credential

PIN

Select another user or provider

Connect a smart card

Connect a smart card

Connect a smart card

sfnt user2
Smart card credential

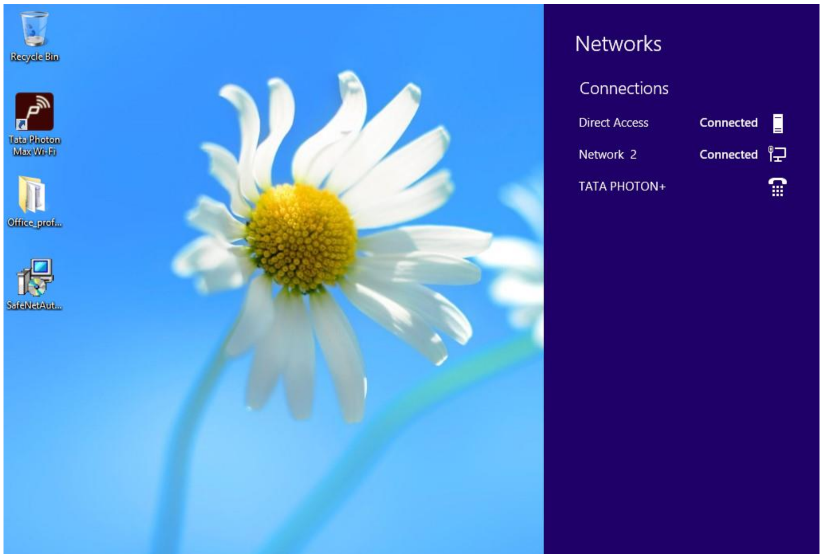
Alice
Smart card credential

No valid certificates were found on this smart card Please try another smart card or contact your

OK Cancel

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

If the credentials are valid, the client machine will connect to DirectAccess.



Networks

Connections

Direct Access	Connected
Network 2	Connected
TATA PHOTON+	

(The screen image above is from Microsoft®. Trademarks are the property of their respective owners.)

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or SafeNet Customer Support. SafeNet Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between SafeNet and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	**Contact Information**	
Address	SafeNet, Inc. 4690 Millennium Drive Belcamp, Maryland 21017 USA	
Phone	United States	1-800-545-6608
	International	1-410-931-7520
Technical Support Customer Portal	https://serviceportal.safenet-inc.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the SafeNet Knowledge Base.	