

Centrify Server Suite 2017

DirectSecure Administrator's Guide

April 2017

Centrify Corporation



• • • • •

Legal notice

This document and the software described in this document are furnished under and are subject to the terms of a license agreement or a non-disclosure agreement. Except as expressly set forth in such license agreement or non-disclosure agreement, Centrify Corporation provides this document and the software described in this document “as is” without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. Some states do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of Centrify Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of Centrify Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. Centrify Corporation may make improvements in or changes to the software described in this document at any time.

© 2004-2017 Centrify Corporation. All rights reserved. Portions of Centrify software are derived from third party or open source software. Copyright and legal notices for these sources are listed separately in the Acknowledgements.txt file included with the software.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government’s rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

Centrify, DirectControl, DirectAuthorize, DirectAudit, DirectSecure, DirectControl Express, Centrify User Suite, and Centrify Server Suite are registered trademarks and Centrify for Mobile, Centrify for SaaS, Centrify for Mac, DirectManage, Centrify Express, DirectManage Express, Centrify Identity Platform, Centrify Identity Service, and Centrify Privilege Service are trademarks of Centrify Corporation in the United States and other countries. Microsoft, Active Directory, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and other countries.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103 B2; 9,112,846; 9,197,670; and 9,378,391.

The names of any other companies and products mentioned in this document may be the trademarks or registered trademarks of their respective owners. Unless otherwise noted, all of the names used as examples of companies, organizations, domain names, people and events herein are fictitious. No association with any real company, organization, domain name, person, or event is intended or should be inferred.

Contents

About this guide

Intended audience	5
Using this guide	5
Conventions used in this guide	6
Finding information about Centrify products	7
Contacting Centrify	7
Getting additional support	7

Chapter 1 How Centrify DirectSecure supports IP security

Introduction to IP security for Windows computers	8
Applying IP security policies to other platforms	9
How DirectSecure uses native and Windows IPsec components	9
Supported authentication modes for DirectSecure	11
How to configure the Public Key Infrastructure on Windows	12
How DirectSecure uses certificates and auto-enrollment	13
IP Security Policies not supported by DirectSecure	14

Chapter 2 Installing Centrify DirectSecure on UNIX

Using existing IP Security Policies	16
Preparing Windows components before installing DirectSecure	17
Preparing Centrify-managed computers	17
Installing Centrify DirectSecure	18
Checking whether IP security policies are deployed	20
Viewing details about the policies deployed	21

Chapter 3 Configuring Centrify DirectSecure

How to configure IP Security Policies	23
Understanding unsupported IP Security features	25



Chapter 4	Troubleshooting DirectSecure and IP Security Policies	
	Common application failures	26
	Using adsec to view IP Security Policies	26
	Addressing warnings returned when you run adsec	31
	DirectSecure Known issues.	40
	Submitting DirectSecure issue details to Centrify Technical Support	42
Chapter 5	Configuring a Linux server for DirectAccess	
	Introduction to Microsoft DirectAccess.	43
	Sample configuration overview	44
	Step 1: Set up the DirectAccess test lab	46
	Step 2: Configure the LINX1 Linux server	46
	Step 3: Configure the DC1 domain controller	48
	Step 4: Verify IPv6 settings	51
	Step 5: Update group policies on LINX1 server	51
	Step 6: Start Apache Web Server	51
	Step 7: Update group policy settings for Client1	52
	Step 8: Verify DirectAccess functionality for Client1	52
Chapter 6	Configuring a Certificate Authority for auto-enrollment	
	Working with a single Certificate Authority for UNIX	53
	Preparing a computer to be a Certificate Authority (CA)	54
	Adding a trusted root certificate to the group policy	56
	Enabling auto-enrollment	57
	Assigning the certificate template to the CA	59
	Understanding how DirectSecure updates CRLs.	59

Index

About this guide

The *Centrify DirectSecure Administrator's Guide* provides information for installing, configuring, and troubleshooting Centrify DirectSecure. Centrify DirectSecure enables you to manage IP Security Policies on UNIX computers using Active Directory group policies. The IP Security Policies protect sensitive information by isolating trusted computers on the network and enabling end-to-end encryption of data in motion.

Intended audience

This guide is intended for network administrators who are responsible for securing communication between trusted computers. The guide assumes that you have a functioning IP Security policies configured for at least one Windows domain. If you do not have IP Security policies configured or are unfamiliar with how to configure Active Directory group policies, you should consult the documentation provided by Microsoft. If you are familiar with Active Directory group policies, group policy objects, and how to configure and apply IP Security policies on Windows computers, this guide notes where DirectSecure IP Security policies differ from the policies defined on Windows.

Using this guide

Depending on your environment and role, you may want to read portions of this guide selectively. The guide provides the following information:

- **Chapter 1, "How Centrify DirectSecure supports IP security,"** provides an overview of IP Security Policy and how Centrify DirectSecure uses the policies defined in Active Directory to provide IP Security on UNIX computers.
- **Chapter 2, "Installing Centrify DirectSecure on UNIX,"** lists the operating system and platform requirements and describes how to install Centrify DirectSecure software on UNIX computers to enable IP Security Policy features.

- Chapter 3, “Configuring Centrify DirectSecure,” summarizes the steps for configuring Active Directory group policies that implement IP Security Policies.
- Chapter 4, “Troubleshooting DirectSecure and IP Security Policies,” explains how to use the `adsec` tool to troubleshoot the DirectSecure implementation of IP Security Policy on a UNIX computer.
- Chapter 5, “Configuring a Linux server for DirectAccess,” explains how to add a Linux server to a Microsoft Windows DirectAccess Test Lab configuration.
- Chapter 6, “Configuring a Certificate Authority for auto-enrollment,” explains how to set up a Certificate Authority to support PKI authentication for Centrify DirectSecure.

In addition to these chapters, an index is provided for your reference.

Conventions used in this guide

The following conventions are used in this guide:

- Fixed-width font is used for sample code, program names, program output, file names, and commands that you type at the command line. When *italicized*, the fixed-width font is used to indicate variables. In addition, in command line reference information, square brackets ([]) indicate optional arguments.
- **Bold** text is used to emphasize commands, buttons, or user interface text, and to introduce new terms.
- *Italics* are used for book titles and to emphasize specific words or terms.
- For simplicity, UNIX is used generally in this guide to refer to all supported versions of the UNIX, Linux, and Macintosh OS X operating systems unless otherwise noted.
- Standalone software packages include version and architecture information in the file name. For example, the standalone software package `centrify-ds-version-rhel4.6-i386.tgz` in documentation refers to a DirectSecure package for Red Hat Enterprise Linux with a file name that includes specific version information, such as `centrify-ds-5.2.1-rhel4.6-i386.tgz`.

Finding information about Centrifly products

Centrifly provides extensive documentation targeted for specific audiences, functional roles, or topics of interest. If you want to learn more about Centrifly and Centrifly products and features, start by visiting the [Centrifly website](#). From the Centrifly website, you can download data sheets and evaluation software, view video demonstrations and technical presentations about Centrifly products, and get the latest news about upcoming events and webinars.

For access to documentation for all Centrifly products and services, visit the [Centrifly documentation portal](#). From the Centrifly documentation portal, you can always view or download the most up-to-date version of this guide and all other product documentation.

To get to the documentation portal, go to docs.centrifly.com or <https://www.centrifly.com/support/documentation>.

Contacting Centrifly

You can contact Centrifly by visiting our website, www.centrifly.com. On the website, you can find information about Centrifly office locations worldwide, email and phone numbers for contacting Centrifly sales, and links for following Centrifly on social media. If you have questions or comments, we look forward to hearing from you.

Getting additional support

If you have a Centrifly account, click Support on the Centrifly website to log on and access the [Centrifly Technical Support Portal](#). From the support portal, you can search knowledge base articles, open and view support cases, download software, and access other resources.

To connect with other Centrifly users, ask questions, or share information, visit the [Centrifly Community](#) website to check in on customer forums, read the latest blog posts, view how-to videos, or exchange ideas with members of the community.

How Centrify DirectSecure supports IP security

This chapter provides an introduction to IP Security Policy for Windows computers and how Centrify DirectSecure extends IP security to protect network traffic on other platforms. The chapter includes an overview of DirectSecure architecture to help you identify the components involved in the application of IP security policies.

The following topics are covered:

- Introduction to IP security for Windows computers
- Applying IP security policies to other platforms
- How DirectSecure uses native and Windows IPsec components
- Supported authentication modes for DirectSecure
- How to configure the Public Key Infrastructure on Windows
- How DirectSecure uses certificates and auto-enrollment
- IP Security Policies not supported by DirectSecure

Introduction to IP security for Windows computers

Internet Protocol security (IPsec) is a low-level protocol for authenticating and encrypting network traffic. The protocol uses cryptographic services to protect communications, encrypting each packet of data that is transmitted over Internet Protocol (IP) networks. The IPsec protocol also supports the establishment of mutual authentication of the beginning of a communication session and ensures the data integrity of transferred during a session.

In an Active Directory environment, IPsec services are deployed and managed through Microsoft IP Security Policies. An administrator configures IP Security Policies through one or more Group Policy Objects (GPO). The administrator can then apply the settings in the Group Policy Objects to a site, domain, or organizational unit. The

Windows domain computers then automatically manage their IP security based on the rules defined in the Group Policy Object.

Applying IP security policies to other platforms

With Centrify DirectSecure, you can use the same approach for applying IP security policies on non-Windows computers as you do on Windows computers. If you have the DirectControl agent installed on a supported operating system for DirectSecure, you simply install DirectSecure on the Centrify-managed computer and use the Windows group policies to configure the IP security rules for the Centrify-managed computer in the same way you do for Windows computers. After you define the rules and apply through a Group Policy Object, Centrify-managed computers automatically manage their IP security based on those rules.

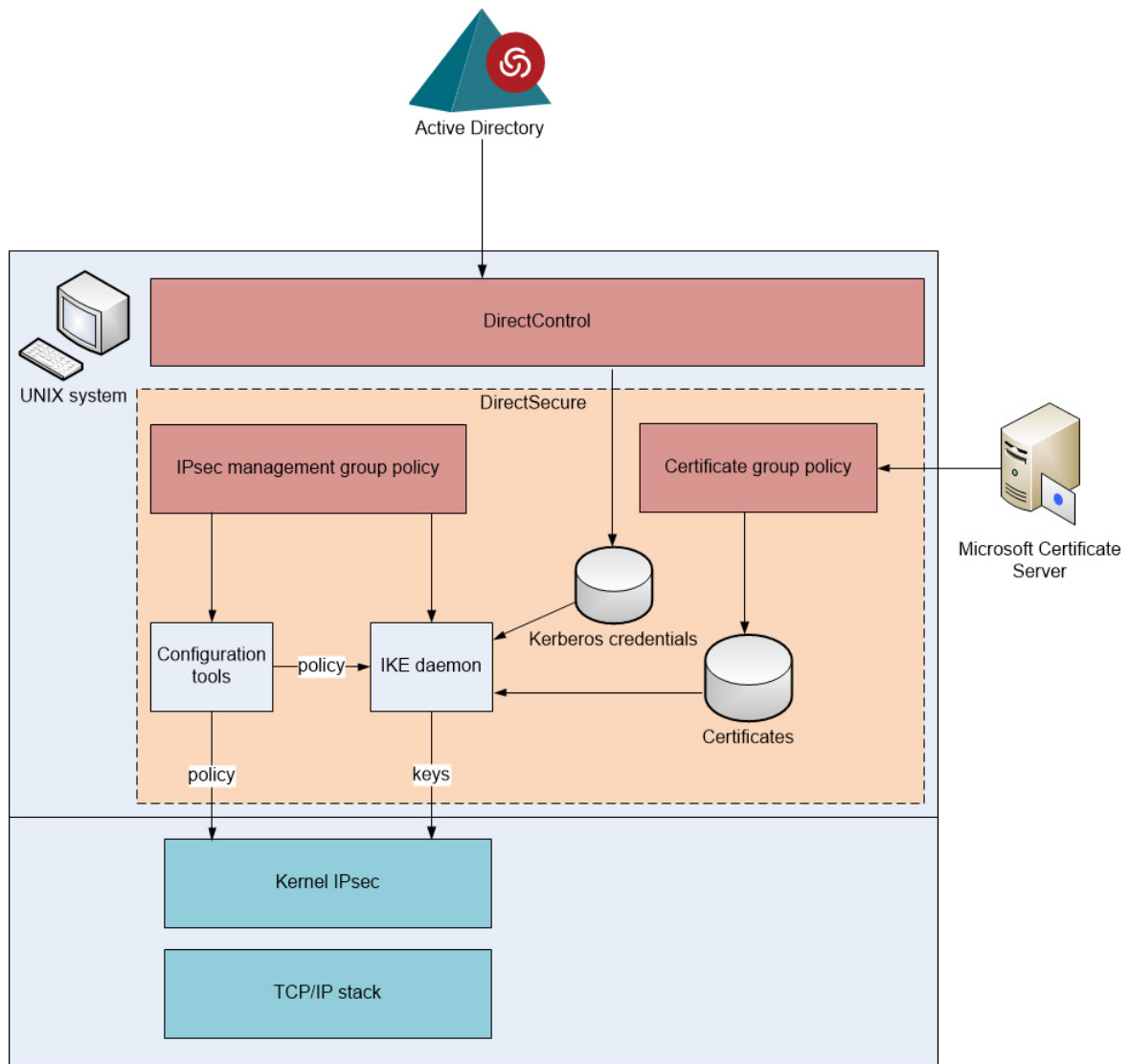
How DirectSecure uses native and Windows IPsec components

The functionality associated with Internet Protocol security (IPsec) is built into the kernel of all the operating systems that support Centrify DirectSecure. However, manually configuring IP security on those platforms using their native IPsec services can be very difficult. To avoid this complexity, Centrify DirectSecure leverages the robust IP Security Policies available on Windows computers.

On Windows, IP security is managed through Active Directory group policies. You use the Group Policy Management Editor to add filters and rules for IP security and deploy those filters and rules to computers through Group Policy Objects. DirectSecure maps the IP Security Policies defined in Active Directory to the native IPsec infrastructure on the non-Windows computers you are managing.

A key component of the IPsec infrastructure is the Internet Key Exchange (IKE) daemon. Most operating systems provide an IKE daemon by default, and DirectSecure provides an IKE daemon for platforms that do not have one. The IKE daemon negotiates key exchanges with the IKE daemon on other computers using the rules and filters you specify. For Centrify DirectSecure, these rules and filters are controlled using group policies and command-line utilities.

The following figure illustrates the Centrif DirectSecure architecture.



Supported authentication modes for DirectSecure

Centrify DirectSecure supports authentication using the following authentication methods:

- Kerberos
- Pre-shared key
- Public Key Infrastructure (PKI)

Kerberos authentication

For Kerberos authentication, Centrify DirectSecure relies on the DirectControl agent. The Centrify agent provides a Kerberos environment that enables existing Kerberos applications to authenticate transparently with Active Directory. For more information about the Centrify agent and the implementation of Kerberos for Linux and UNIX computers, see the *Administrator's Guide for Linux and UNIX*.

Pre-shared key authentication

Microsoft Windows stores pre-shared keys in Active Directory. If a computer is configured with IP Security Policies that use pre-shared keys for authentication, all of the information for the keys is downloaded when the computer joins a domain. For example, for the `racoon` IKE daemon, the pre-shared key information is stored in the file `/etc/centrifydc/racoon/psk.conf`, which is protected with root file permissions.

Note Microsoft recommends using **pre-shared keys** for testing only. For production environments, you should use PKI or Kerberos V5, both of which are supported by Centrify DirectSecure.

Public Key Infrastructure (PKI) authentication

Microsoft Windows provides a Public Key Infrastructure (PKI) that Centrify DirectSecure uses to obtain certificates and install them on Centrify-managed computers that are joined to a domain.

DirectSecure supports the use of certificates that use an RSA algorithm or an Elliptic Curve Cryptography (ECC) algorithm.

Note Certificates that use the Elliptic Curve Cryptography (ECC) algorithm can be used for IPsec authentication between UNIX computers or between Windows computers. ECC certificates aren't supported yet for IPsec authentication between a UNIX computer and a Windows computer.

For an overview of how to configure the Microsoft Windows PKI components required for PKI authentication, see [“How to configure the Public Key Infrastructure on Windows” on page 12](#). For an overview of how DirectSecure uses the [certificate auto-enrollment feature](#) to make certificates available to Centrify-managed computers, see [“How DirectSecure uses certificates and auto-enrollment” on page 13](#).

For more detailed instructions on how to configure PKI components for DirectSecure, see [Chapter 6, “Configuring a Certificate Authority for auto-enrollment.”](#)

How to configure the Public Key Infrastructure on Windows

Before you can use PKI authentication with DirectSecure, you must configure the appropriate components on Windows computers. For example, DirectSecure requires an Active Directory domain controller to be configured as the Certification Authority (CA) server for the Active Directory forest. Other certificate issuers are not currently supported.

The following steps summarize the process for configuring PKI on Windows:

- 1 Identify an Active Directory domain controller to act as the **Certificate Authority** for the enterprise.

Active Directory services must be available on the computer that issues certificates.

- 2 Install **Internet Information Services (IIS)** and **Certificate Services** on the domain controller.

- Microsoft Internet Information Services (IIS) handle Certificate Revocation List (CRL) requests made by DirectSecure and provide the virtual directories required to issue and manage certificates.
 - Certificate Services are required to enable the computer to act as a Certificate Authority (CA) and issue certificates to other computers. The Application server role, which installs IIS, and the Certificate Services server role must be on the same computer.
- 3 Add a trusted root certificate to the group policy.

To establish a chain of trust for the PKI environment, you must identify an entity, such as the root CA, as a trust anchor. You can establish the CA as a trust anchor by adding the CA's root certificate to the **Trusted Root Certification Authorities** container in the group policy object that defines the IP Security Policies.

- 4 Enable auto-enrollment for the group policy.

If you specify auto-enrollment for public key policies, computers associated with the group policy object automatically enroll for certificates.

- 5 Create a certificate template with auto-enrollment permission and assign it to the CA.

You must create a certificate template and assign it to a CA. The CA generates certificates to be downloaded by DirectSecure based on the certificate template you assign. This template must have auto-enrollment permission enabled.

How DirectSecure uses certificates and auto-enrollment

Centrify DirectSecure makes the certificates required for PKI authentication available to Centrify-managed computers through the auto-enrollment and certificate templates.

Microsoft Windows stores certificate templates in a global location in Active Directory. When a computer joins a domain, DirectSecure locates the templates in Active Directory. For each template that is configured for auto-enrollment, DirectSecure determines whether a

certificate has been issued and installed on the joined computer, and if not, contacts the Certificate Authority (CA) using Kerberos credentials to obtain one.

During this process, DirectSecure checks the certificates that have already issued to make sure they are still valid—that is, the certificates have not expired and have version numbers that match their related certificate template—and requests them to be reissued, if needed.

By default, DirectSecure installs the certificate, its private key, and the certificate trust chain in the following directory:

```
/var/centrify/net/certs
```

DirectSecure uses the trust chain to extract the CA root certificates and installs them in a location where the IKE daemon can read them (`/var/centrify/net/certs` by default).

DirectSecure downloads the Certificate Revocation List (CRL) from the CA server to identify certificates that are no longer valid. DirectSecure also fetches CRLs based on the CRL URLs in any certificates it needs to check as part of a key exchange negotiation with another computer.

In addition to using CRLs, DirectSecure uses the [Online Certificate Status Protocol \(OCSP\)](#), to determine the status of a certificate.

Note Centrify DirectSecure supports sending and receiving PKCS7 certificate bundles, which are useful in a multi-tiered Certificate Authority infrastructure. For example, a computer only needs to be configured to trust the root CA because the PKCS7 bundle allows the computer to follow the chain from the certificate to the root authority.

IP Security Policies not supported by DirectSecure

IP security supports two modes of network connections: tunnel and transport. Tunnel is typically used to implement VPN functionality and is not supported by Centrify DirectSecure. DirectSecure only supports transport mode, which is used for host-to-host communications.

There are also a few Windows-specific IP Security Policy settings that are not implemented by Centrify DirectSecure. However, the

differences between Windows IP Security Policies and the DirectSecure IP security implemented are minor. In most cases, you can create the same filters and apply the same rules for non-Windows computers that you can for Windows computers.

Note DirectSecure does not support the use of IPsec protocols to encrypt network traffic between a computer running DirectSecure and a domain controller when the IP Security Policies are applied through a Group Policy Object. This limitation is not unique to DirectSecure. It is a built-in limitation that prevents the encryption of network traffic from a Windows domain computer to a domain controller that has IP Security Policies applied. For more information about this limitation, see the Microsoft Support article [IPsec support for client-to-domain-controller traffic](#).

Installing Centrify DirectSecure on UNIX

This section provides step-by-step instructions for installing Centrify DirectSecure on UNIX computers.

The following topics are covered:

- Using existing IP Security Policies
- Preparing Windows components before installing DirectSecure
- Preparing Centrify-managed computers
- Installing Centrify DirectSecure
- Checking whether IP security policies are deployed
- Viewing details about the policies deployed

Using existing IP Security Policies

Before you install Centrify DirectSecure, you should have a Windows environment in which you have configured IP Security Policies for Windows computers and verified that the policies are working as expected. If you have previously configured Active Directory group policies and IP security methods and filters on Windows computers, you can expect a successful deployment of DirectSecure with little or no additional configuration.

If you do not have IP Security Policies configured for Windows computers, you should contact the Active Directory administrator to prepare the environment with the appropriate group policy settings, group policy objects (GPOs), and links, before installing DirectSecure.

Preparing Windows components before installing DirectSecure

Centrify DirectSecure does not require you to install any additional components on Windows systems. However, DirectSecure does require you use the Group Policy Management Editor to configure IP Security Policies, and optionally, a Certificate Authority (CA) server to issue certificates for authentication.

To prepare for deploying IP Security Policies for non-Windows computers, you should check that your environment meets the following basic requirements.

For this component	DirectSecure requires
Domain controllers	One of the following platforms: <ul style="list-style-type: none">• Windows Server 2008• Windows Server 2012 or 2012 R2
Certificate Services	A Windows computer with a Certificate Authority (CA) server role and Certificate Services: <ul style="list-style-type: none">• Windows Server 2008• Windows Server 2012 or 2012 R2 Certificate Services are required if you want to use encrypted certificates for authentication, which is the recommended configuration.

Preparing Centrify-managed computers

Before you install DirectSecure on a computer, make sure that the computer meets the following requirements:

- The computer has an operating system version that is supported for use with DirectSecure.

For detailed information about the operating systems and versions supported for the version of DirectSecure you are installing, see the [Centrif web site](#).

- You can log on to the console.
- You can log on as root.
- There are no other IPsec implementations running on the computer.
- The DirectControl agent is installed and matches the version of DirectSecure that you are installing.

For example, if you are installing DirectSecure version 5.2.0, you should be sure that the Centrif agent you have installed is version 5.2.0.

You can use `adinfo -v` to verify the version of the Centrif agent you have installed.

Installing Centrif DirectSecure

Centrif DirectSecure files are delivered in platform-specific software packages. You can install the software using the native package installer for each platform or using another package management program, such as SMIT or YAST. You must install the DirectSecure package on each computer that will be configured for IP security.

To install Centrif DirectSecure on a computer:

- 1 Log on as or switch to the `root` user.
- 2 If you are installing from a CD and the CD drive is not mounted automatically, use the appropriate command for the local computer's operating environment to mount the `cdrom` device.
- 3 Download or locate the software package for the specific operating system of the computer for which you want to define IP security policies.

For example, if the operating environment is Red Hat Enterprise Linux, the DirectSecure package might be `centrif-ds-release-rhel4.6-i386.tgz`.

- 4 Unzip and extract the software package using the appropriate commands for the local operating system.

For example, you might run the following commands if the operating system is Red Hat Enterprise Linux:

```
gunzip -d <centrify-directsecure-package>.tgz  
tar -xf <centrify-directsecure-package>.tar
```

- 5 Install the DirectSecure package.

For example, you can use Red Hat Package Manager (`rpm`) to install on Red Hat Enterprise Linux and SuSE Linux:

```
rpm -Uvh <centrify-directsecure-package>.rpm
```

On Solaris computers, run these commands:

```
gzip -d <centrify-directsecure-package>.tgz  
tar -xvf <centrify-directsecure-package>.tar  
pkgadd -d CentrifyDS
```

On Debian computers, run this command:

```
dpkg -i <centrify-directsecure-package>.deb
```

- 6 Verify that DirectSecure is installed.

- On SUSE Linux and RHEL computers:

```
rpm -qa CentrifyDS
```

As a result, you should see something like this:

```
CentrifyDS-<release>
```

- On Solaris computers:

```
pkginfo -l CentrifyDS
```

As a result, `pkginfo` should show status of `completely installed`.

- On Debian computers:

```
dpkg -l | grep centrifyds
```

As a result, you should see something like this:

```
centrifyds-<release>
```

Installing DirectSecure on Solaris computers with zones

For zones that have their own physical network interface cards, you can install DirectSecure in them according to the install instructions mentioned in the previous section. Each zone is effectively treated as a separate, virtual computer.

For zones that have virtual network interface cards, such as where the Global Zone provides the network interface, don't install DirectSecure in the zone. Instead, install DirectSecure in the Global Zone (use the `pkgadd` command with the `-G` option). An installation in the Global Zone provides DirectSecure services for all zones for which the Global Zone provides a network interface.

Uninstalling DirectSecure

If you need to uninstall DirectSecure, run one of the commands below.

- On SUSE or RHEL computers:

```
rpm -e CentrifysDS
```

- On Solaris computers:

```
pkgrm CentrifysDS
```

- On Debian computers:

```
dpkg -P centrifysds
```

Checking whether IP security policies are deployed

If you have previously configured a Group Policy Object with IP security methods and filters and applied the GPO to the Active Directory site or a domain the non-Windows computer is part of, those policies can be inherited without further configuration. After you have installed the DirectSecure package, you can use the `adsec` command to check whether Centrifys DirectSecure is installed and currently running.

For example, to see if there are IP security policies applied on the local computer, run the following command:

```
adsec --status
IKE service ... running
```

If the IKE service is running, you can establish secure communications between the local computer and the following types of Windows computers:

- Windows 7 or later
- Windows 8 or 8.1
- Windows 2008 or 2008 R2
- Windows Server 2012 or 2012 R2

You cannot encrypt network traffic between a computer running DirectSecure and a domain controller when security policies are applied through a Group Policy Object on a domain controller. For information about this limitation, see the Microsoft Support article, [IPsec support for client-to-domain-controller traffic](#).

Viewing details about the policies deployed

If the `adsec --status` command indicates that the IKE service is currently running, there are IP security policies assigned to the local computer. To see details about the policies that have been assigned, run the following command:

```
adsec --policy
-----
Machine IP addresses used for "My Address" in IPsec rules:
    192.168.43.133
-----
Policy: Client (Respond Only)
IKE settings
    PFS: 0
    Options: 0
    QMLimit: 11
Phase 1 SA settings
    3des / sha1 / dh-2 life(secs):28800
```

```
3des / md5 / dh-2 life(secs):28800  
des / sha1 / dh-1 life(secs):28800
```

```
-----  
Rule 0() active  
Warning: MS default rules are not supported. skipping rule  
-----
```

If the `adsec --status` does not return a running status, there are no IP security policies currently assigned to the local computer. For information about configuring IP security policies for the computer, see [“Configuring Centrify DirectSecure” on page 23](#).

Configuring Centrify DirectSecure

This chapter explains how to configure IP Security Policies as implemented by Centrify DirectSecure.

The following topics are covered:

- [How to configure IP Security Policies](#)
- [Understanding unsupported IP Security features](#)

How to configure IP Security Policies

After you have installed Centrify DirectSecure on Centrify-managed computers that are joined to an Active Directory domain, you configure IP Security Policies for those computers exactly as you do for Windows computers in the domain. You configure the rules and filters by setting IP Security Policies in a Group Policy Object. You can then apply the Group Policy Object to a site, domain, or organizational unit that includes the Centrify-managed computers.

For more information about configuring group policies, editing Group Policy Objects, and applying Group Policy Objects, see the *Centrify Server Suite Group Policy Guide*.

To configure IP Security Policies for Centrify-managed computers:

- 1 Verify that port 135 is open on your Active Directory domain controllers to allow TCP communication.
- 2 Install DirectSecure on computers in the domain as described in [“Installing Centrify DirectSecure” on page 18](#).
- 3 Open the Group Policy Management console and expand the domains or organizational units to locate the Group Policy Objects you have deployed and where they are applied.

For example, select the Default Domain Policy or the Default Domain Controllers Policy, then click the **Scope** and **Settings** tabs

to see details about the settings you have defined for those Group Policy Objects.

- 4 Select an existing Group Policy Objects or right-click a domain or container to create a new Group Policy Object.
- 5 Right-click the Group Policy Object, then click **Edit**.
- 6 In the Group Policy Management Editor, expand **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies on Active Directory**.
- 7 Select **Secure Server (Require Security)**, right-click, then click **Properties** to review specific IP Security Policies you have defined for Windows computers.

If your Centrify-managed computers are on the same subnets as your Windows computers and you want to apply the same IP Security Policies to them, no additional configuration is necessary. The IP Security Policies rules you have defined for Windows will apply automatically to the Centrify-managed computers.

If the Centrify-managed computers are on different subnets than the Windows computers, you must define new IP Security Policies for them.

- 8 Right-click **IP Security Policies for Active Directory**, then click **Create IP Security Policy** to create a new IP Security Policy for Centrify-managed computers.
- 9 Follow the prompts displayed in the wizard to create the new IP Security Policies to enforce.
- 10 On the UNIX computer where you installed Centrify DirectSecure, run the `adsec --policy` command to verify the IP Security Policies configuration.

If you see error or warning messages in the output from `adsec`, see [“Addressing warnings returned when you run adsec” on page 31](#) for more information about the problems found.

Understanding unsupported IP Security features

After you define IP Security Policies, those IP Security Policies can apply to both Windows and Centrify-managed computers. In most cases, DirectSecure enforces the IP Security Policies exactly as they are defined for Windows computers. However, there are a few IP Security Policies that differ slightly when they are applied to Windows from when they are applied on Centrify-managed computers. There are also a few specific IP Security Policies that are not supported for Centrify-managed computers.

You can use the `adsec --policy` command to see details about the active IP Security Policies, including any Windows configuration settings that cannot be implemented on Centrify-managed computers. You should run this command to verify your IP Security Policies configuration, especially if you want to apply the same IP Security Policies to both Windows and Centrify-managed computers.

Troubleshooting DirectSecure and IP Security Policies

This chapter explains how to troubleshoot the IP Security Policies as implemented by Centrify DirectSecure.

The following topics are covered:

- Common application failures
- Using `adsec` to view IP Security Policies
- Addressing warnings returned when you run `adsec`

Common application failures

Certain command-line programs—such as `ftp` and `ping`—may fail the first time you use them after installing DirectSecure. In most cases, this failure is temporary and the applications will run successfully after a short delay.

The reason some applications fail initially is because they were originally written before IP security was developed. The first time you execute a command such as `ping`, there are no security associations (SAs) for the communication, so the kernel requests an SA from the IKE daemon and issues `EAGAIN` to the `ping` command so it will try again. However, on some platforms, the command simply fails, rather than executes again. In this case, if you issue the command again, the SA has probably been created and the command should succeed.

Using `adsec` to view IP Security Policies

You can use the `adsec` command line program to display information about the currently defined IP Security Policies and any policies that cannot be implemented due to platform restrictions. You can also use the `adsec` command to manage IP security settings on a Centrify-managed computer.

The basic syntax for `adsec` is:

```
adsec [--certs] [--debug [on | off]] [--disable] [--enable]
[--flush [sa | sp | all]] [--ikeinfo] [--info] [--policy]
[--reload] [--reset] [--sainfo] [--spinfo] [--status] [--
stop] [--support] [--unconfig] [--version]
```

Setting valid options

You can use the following options with this command:

Use this option	To do this
<code>--certs</code>	Display information about the certificates stored in the <code>/var/centrify/net/certs</code> directory. This option also performs a basic test to verify that the public key information stored in each certificate matches the private key data stored in the associated key file.
<code>--debug on off</code>	Turn debugging on or off. The default, if you do not specify this parameter, is off. Debugging information is sent to the <code>/var/log/centrify-racoon.log</code> file. Turning on debugging with this parameter, sets <code>racoon</code> debugging to verbose and updates the <code>/etc/sysconfig/centrify-racoon</code> configuration file with changes to <code>RACOOON_OPTS</code> .
<code>--disable</code>	Suspend processing of IP Security Policies to allow you to make manual changes to the policy. Note that manual changes are overwritten when group policy processing is re-enabled.
<code>--enable</code>	Enable the processing of IP security policies. By default, policy processing is enabled. Use this option to re-enable IP security policies after suspending them with the <code>--disable</code> option.
<code>--flush sa sp all</code>	Flush the Security Authority (<code>sa</code>) database, the Security Policy (<code>sp</code>) database, or both (<code>all</code>). These databases hold the security authority and security policy information. If these policies are not working as expected, for example, if they are restricting traffic with the domain controller, flushing the policies allows easy recovery.
<code>--ikeinfo</code>	Display the state of IKE negotiation with its peers.

Use this option	To do this
<code>--info</code>	Display the state of group policy management and whether group policy management of IP Security Policies is enabled or disabled on the computer.
<code>--policy</code>	Print a readable version of the IP security policies to standard output, including any errors or warnings that were generated. See “Examples of using adsec” on page 29 for a list of IP security policies errors reported by the <code>--policy</code> option.
<code>--reload</code>	Flush the Security Authority and Security Policy databases, then reload the information from the <code>racoon spd.conf</code> file.
<code>--reset</code>	Restart the <code>IKE</code> daemon.
<code>--sainfo</code>	List information about the active security associations.
<code>--spinfo</code>	List security policy information, including source and destination addresses, direction, protocols to control, and the rules to apply.
<code>--status</code>	Show the status of the <code>IKE</code> daemon.
<code>--stop</code>	Stop the <code>IKE</code> daemon.
<code>--support</code>	Generate a compressed archive file containing information that can be used by customer support to troubleshoot the IP security policies, including: <ul style="list-style-type: none"> • The <code>IKE</code> configuration file • The current Security Policy Database (SPD) configuration • The <code>IKE</code> log file, which is located in <code>/var/log</code>. The name of the log file will vary depending on the <code>IKE</code> daemon, which may be provided by the operating system or installed by DirectSecure. <p>The compressed archive file is created as <code>/var/centrify/tmp/centrify_ipsec_tar.gz</code>.</p>

Use this option	To do this
<code>--unconfig</code>	Remove the configuration settings. This setting is primarily used by the package scripts so that the package can be uninstalled. If you run <code>adsec --unconfig</code> by mistake, you can run the <code>adgpupdate</code> command to reconfigure the DirectSecure service again.
<code>--version</code>	Display version information for <code>adsec</code> .

Examples of using adsec

In most cases, you use `adsec` to provide information that you can use to diagnose and resolve problems with the configuration of IP Security Policies.

The `--policy` option prints to standard output details of the IP Security Policies on Active Directory configuration. Included in the output are warnings and error messages for any settings that cannot be implemented or are ignored by DirectSecure.

Note The `adsec --policy` command retrieves information about the IP Security Policies directly from Active Directory, not from the configuration files on the managed computer. If you run `adsec --policy` immediately after making changes to group policies in Active Directory, the command output will show any changes that were made, but the changes will not be written to the configuration files on the managed computer until the next refresh interval (default is 8 hours). You can force a refresh of the IP Security Policies on a computer by running the `adgpupdate` command.

The following example shows the configuration for one of the Windows default policies, **Secure Server (Require Security)**:

```
adsec --policy
-----
-----
Machine IP addresses used for "My Address" in IP Security
Policy rules:
    192.168.43.133
```

```
-----  
-----  
Policy: Secure Server (Require Security)  
IKE settings  
  PFS: 0  
  Options: 0  
  QMLimit: 0  
Phase 1 SA settings  
  3des / sha1 / dh-2 life(secs):28800  
  3des / md5 / dh-2 life(secs):28800  
  des / sha1 / dh-1 life(secs):28800  
Warning: Diffie-Hellman group: dh-1 is different from the  
first security method offer, dh-2 will be used instead  
  des / md5 / dh-1 life(secs):28800  
Warning: Diffie-Hellman group: dh-1 is different from the  
first security method offer, dh-2 will be used instead  
-----  
-----  
Rule 0(All ICMP Traffic) active  
  Authorization Modes:  
    krb5 /  
  Policy:  
    Action: ipsec esp/transport//unique  
Warning: Changing policy action from inbound pass through  
to secure  
  SA offers:  
    Lifetime(secs): 900  
    Lifetime(KB): 100000  
    Use PFS): no  
    3des / sha1 / esp  
    3des / md5 / esp  
    des / sha1 / esp  
    des / md5 / esp  
  Filters:  
    My Address -> Any Address mirror:y  
protocol:icmp  
-----  
-----  
Rule 1() active
```

```
Warning: MS default rules are not supported. skipping rule
-----
-----
Rule 2(All IP Traffic) active
  Authorization Modes:
    krb5 /
  Policy:
    Action: ipsec esp/transport//unique
Warning: Changing policy action from inbound pass through
to secure
  SA offers:
    Lifetime(secs): 900
    Lifetime(KB): 100000
    Use PFS): no
    3des / sha1 / esp
    3des / md5 / esp
    des / sha1 / esp
    des / md5 / esp
  Filters:
    My Address          -> DNS Server          mirror:y
protocol:any
Warning: Destination address set to DNS server is not
supported. skipping filter
-----
-----
```

Addressing warnings returned when you run adsec

This section lists the warnings and errors related to the specific IP Security Policies that are not supported or not fully supported by Centrify DirectSecure. If you run the `adsec --policy` command on a managed computer and see any errors or warnings, this section describes where you can find the related feature in IP Security Policies group policy configuration, how to correct the error, and the consequences of leaving the setting unchanged.

- **Warning: MS default rules are not supported**

- Warning: Diffie-Hellman group
- Warning: Destination address is not supported
- Warning: Lifetime (secs)
- Warning: Mixing ESP and AH is not supported
- Warning: Changing policy action from inbound pass through to secure

Warning: MS default rules are not supported

When you configure IP Security Policies, you can activate a default response rule. The default response rule responds to remote computers that request secure communication when no other rule applies. DirectSecure ignores this setting. However, if you create an IP Security Policies with rules for all situations, ignoring the default response rule does not leave any holes in your IP security.

Symptom

If you have configured IP Security Policies with the **Activate default response rule** option selected and that policy is applied to Centrify-managed computers, the `adsec --policy` command displays the following message:

```
Warning: MS default rules are not supported. Skipping rule
```

Solution

Leaving the **Activate default response rule** option selected has no affect on your IP Security Policies for Centrify-managed computers other than you see a warning whenever you run `adsec --policy`. However, you should be aware that the computer does not have an active default response rule to fall back to if no other rules apply.

If you want to change the setting that generates the warning message, do the following:

- 1 Select the group policy object to edit and navigate to the IP Security Policies. For example, select **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies** in the Group Policy Management Editor.

- 2 Select the IP security policy to edit, right-click, then click **Properties**.

If you have not previously created IP Security Policies or do not want to edit an existing one, right-click, then click **Create IP Security Policy** and follow the prompts displayed to specify the name and description of the policy. When prompted for **Requests for Secure Communication** do not select **Activate the default response rule**.

- 3 On the Rules tab, uncheck the **Default response** IP filter option, then click **OK**.

Warning: Diffie-Hellman group

When you configure IP Security Policies, you configure the security methods used to protect identities during key exchange. Typically, you configure multiple methods that have different encryption strengths so that you can accommodate connections with a range of computers that have different requirements.

When you are configuring the properties for the Key Exchange Security Methods, you list the methods in the order to use when negotiating the key exchange with another computer. For each method, you must also specify the level — low (1), medium (2), or high (3) — for the Diffie-Hellman groups. Diffie-Hellman groups form the basis for creating future keys.

If you specify different Diffie-Hellman levels for the encryption methods allowed, Windows-to-UNIX or UNIX-to-Windows connections may fail. However, Windows-to-Windows connections and UNIX-to-UNIX connections should work as expected.

Symptom

If you have configured IP Security Policies with different Diffie-Hellman levels assigned to different security methods and that policy is applied to Centrify-managed computers, the `adsec --policy` command displays a message similar to the following:

```
Warning: Diffie-Hellman group: dh-1 is different from the
first security method offer, dh-2 will be used instead
```

Solution

If you want to change the setting that generates the warning message, do the following:

- 1 Select the group policy object to edit and navigate to the IP Security Policies. For example, select **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies** in the Group Policy Management Editor.
- 2 Select the IP security policy to edit, right-click, then click **Properties**.
- 3 Click the **General** tab, then click **Settings**.
- 4 In the Key Exchange Setting dialog box, click **Methods**.
- 5 Configure all of the methods listed in the Key Exchange Security Methods to use the same Diffie-Hellman level, then click **OK**. Using the same level for all methods ensures that no connection errors occur during the Internet Key Exchange (IKE) process.

Warning: Destination address is not supported

When creating a filter list for the source or destination address, you can select a server type—for example DNS, WINS, DHCP, or Default Gateway—instead of a specific or general IP address. DirectSecure ignores these settings.

Symptom

If you have configured an IP security policy with DNS, WINS, DHCP, or Default Gateways filters and that policy is applied to Centrify-managed computers, the `adsec --policy` command displays a message similar to the following:

```
Warning: Destination address set to serverType server is not supported. skipping filter
```

where *serverType* is one of: DNS, WIND, DHCP, Default Gateway

Solution

If you want to change the setting that generates the warning message, do the following:

- 1 Select the group policy object to edit and navigate to the IP Security Policies. For example, select **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies** in the Group Policy Management Editor.
- 2 Select the IP security policy to edit, right-click, then click **Properties**.
- 3 On the **Rules** tab, uncheck the **Use Add Wizard** option, then click **Add**.
- 4 On the IP Filter List tab, select an IP Filter, then click **Edit**.
- 5 Click Edit to display the IP Filter Properties.
- 6 Change the Source or Destination address that specifies a server type, such as DNS Servers, to **A specific IP Address or Subnet**, then type the IP address for a specific server type, such as the DNS server.

Warning: Lifetime (secs)

When you configure IP Security Policies, you can define multiple security methods in an ordered list to accommodate connection to computers with different security capabilities. For each method, you can specify the lifetime of the key in kilobytes, in seconds, or in both.

DirectSecure does not support the kilobytes setting—it is ignored. For DirectSecure, the key lifetime must be specified in seconds.

If the number of seconds for the key lifetime differs for any of the security methods for any given filter action, Windows-to-UNIX connections or UNIX-to-Windows connections may fail. However, Windows-to-Windows and UNIX-to-UNIX connections should work as expected.

Symptom

If you have configured IP Security Policies with different lifetime values assigned to different security methods or specified the lifetime in KB instead of seconds and that policy is applied to Centrify-managed computers, the `adsec --policy` command displays a message similar to the following:

```
Warning: Lifetime(secs):600 is different from the first SA offer, 900 will be used instead
```

Solution

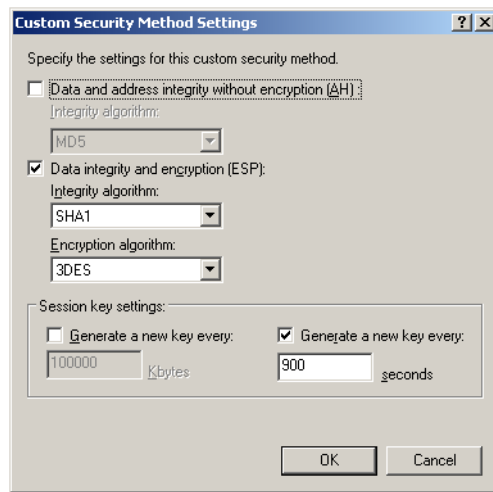
If you want to change the setting that generates the warning message, do the following:

- 1 Select the group policy object to edit and navigate to the IP Security Policies. For example, select **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies** in the Group Policy Management Editor.
- 2 Select the IP security policy to edit, right-click, then click **Properties**.
- 3 On the **Rules** tab, uncheck the **Use Add Wizard** option, then click **Add**.
- 4 Click the **Filter Action** tab.
- 5 Select a filter action, such as **Require Security**, then click **Edit**.
- 6 Check the Key Lifetime for each security method and configure the value in seconds to be the same for all methods.

To change the lifetime for a new key:

- Select a method in the list, then click **Edit**.
- Select **Custom**, then click **Settings**.

- Set a new value for the number of seconds, then click **OK**. The Kbytes setting is ignored whether you check it or not.



Warning: Mixing ESP and AH is not supported

When you configure IP Security Policies, you can define multiple security methods in an ordered list to accommodate connections to computers with different security capabilities. For each security method, you can select **Data and address integrity without encryption (AH)** or **Data integrity and encryption (ESP)**. However, for any given filter action, if you mix AH and ESP for the security methods, Windows-to-UNIX connections or UNIX-to-Windows connections may fail. However, Windows-to-Windows and UNIX-to-UNIX connections should work as expected.

Symptom

If you have configured IP Security Policies with security methods that have a mix of data integrity with and without encryption and that policy is applied to UNIX computers, the `adsec --policy` command displays a message similar to the following:

```
Warning: Mixing ESP and AH in the same SA is not supported,  
ESP will be used instead
```

Solution

If you want to change the setting that generates the warning message, do the following:

- 1 Select the group policy object to edit and navigate to the IP Security Policies. For example, select **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies** in the Group Policy Management Editor.
- 2 Select the IP security policy to edit, right-click, then click **Properties**.
- 3 On the **Rules** tab, uncheck the **Use Add Wizard** option, then click **Add**.
- 4 Click the **Filter Action** tab, select an IP Filter, then click **Edit**.
- 5 Select a filter action, such as **Require Security**, then click **Edit**.
- 6 Configure AH or ESP for all methods in the list to avoid potential connection problems between UNIX and Windows computers.

To change the data integrity and encryptions settings:

- Select a method in the list, then click **Edit**.
- Select **Custom**, then click **Settings**.
- Select the appropriate data integrity and encryption options to make all security methods consistent, then click **OK**.

Warning: Changing policy action from inbound pass through to secure

When you configure IP Security Policies, the following two settings work together to determine the fallback IP security policy:

- **Accept unsecured communication, but always respond using IP Security Policy** specifies whether inbound traffic must be secure.
- **Allow fallback to unsecured communication if a secure connection can not be established** specifies whether outbound traffic must be secure.

DirectSecure supports any combination of these settings, except turning off the first (leaving it unchecked) and turning on the second.

```
[ ] Accept unsecured communication, but always respond using IPsec
```

```
[X] Allow fallback to unsecured communication if a secure connection can not be established
```

For DirectSecure, turning off the first setting and turning on the second setting, is the same as turning both off.

Symptom

If you have configured IP Security Policies with the unsupported inbound and outbound settings, the `adsec --policy` command displays a message similar to the following:

```
Warning: Changing policy action from inbound pass through to secure
```

Solution

If you want to change the setting that generates the warning message, do the following:

- 1 Select the group policy object to edit and navigate to the IP Security Policies. For example, select **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies** in the Group Policy Management Editor.
- 2 Select the IP security policy to edit, right-click, then click **Properties**.
- 3 On the **Rules** tab, uncheck the **Use Add Wizard** option, then click **Add**.
- 4 Click the **Filter Action** tab.
- 5 Select a filter action, such as **Require Security**, then click **Edit**.
- 6 Check the selections for unsecured communication.
 - If **Accept unsecured communication, but always respond using IP Security Policy** is not selected, you should verify that **Allow fallback to unsecured communication if a secure connection can not be established** is also not selected.

- If **Allow fallback to unsecured communication if a secure connection can not be established** is selected, you should verify that **Accept unsecured communication, but always respond using IP Security Policy** is also selected.

For DirectSecure, if secure inbound traffic is required, secure outbound traffic is also required.

DirectSecure Known issues

There are some known issues when deploying and using DirectSecure. Some of these issues have workarounds.

Fails to connect due to time out

Symptom When trying to connect from a Solaris machine to another UNIX machine after applying IPsec group policy (for example, using ssh), the connection may fail with a time-out.

Explanation The reason why this happens is that Solaris does not work properly with 'non-mirror' or 'any protocol' settings in the IPsec policy (Ref: DS-521, DS-438).

Computers on which IPsec policy allows only ICMP traffic are not always able to ping

Symptom If the effective IPsec policy allows ICMP traffic only (no UDP or TCP traffic allowed), Windows computers can ping UNIX computers, but UNIX computers cannot ping Windows computers.

The problem is caused by the Linux implementation of ping; it does a UDP bind to the remote machine and this causes IPsec to establish SAs, even though they are not needed.

Solution: In these situations, ping a Windows computer from a UNIX computer by running the following command

```
ping -I <my ip address> <remote ip address>
```


Certificate principal mapping is not supported

Certificate principal mapping ensures that the computer is known to Active Directory before accepting certificates. This feature is not supported.

Certificate-based IPsec to the CA is not supported

Usually, customers allow unrestricted access to a certificate authority (CA) system. Although it is possible to configure certificate-based IPsec authentication to the CA (for example, you can do this by specifying a subnet-wide policy without exclusions), this configuration is not supported in environments with only Microsoft Windows computers (no UNIX/Linux computers).

Restarting centrify-racbridge and centrify-racoon services on Solaris (Ref: DS-449)

Symptom "The `svcadm restart centrify-racbridge` command does not start the centrify-racbridge and centrify-racoon services in proper order.

Solution: Use the `adsec -r` command instead.

CertGP takes a long time and can get aborted on Solaris (Ref: IN-90001)

Symptom DirectSecure implements PKI certificate handling as a group policy, and the DirectControl Group Policy Mapper runs the PKI certificate handling.

On Solaris computers, the CertGP group policy takes longer to run than on other platforms and can run longer than the default timeout value associated with DirectControl group policies; as a result, the CertGP is aborted.

Solution: Increase the DirectControl group policy timeout value and restart DirectControl.

To increase the default timeout value for DirectControl group policies on Solaris computers:

- 1 Open this file: `/etc/centrifydc/centrifydc.conf`.
- 2 Locate this property:
`# gp.mappers.timeout: 30`
- 3 Uncomment the line (remove the "# " at the beginning) and change the value to 60.
- 4 Save the file.
- 5 Restart DirectControl by running the following command:
`/usr/share/centrifydc/bin/centrifydc restart`

Submitting DirectSecure issue details to Centrify Technical Support

If a problem occurs, please send a problem description to support@centrify.com. To improve the speed of resolution, please include information about the system and version of software you are using. One way of doing it is to run the following commands and paste the output into the report.

For SUSE or RHEL computers:

```
hostname ; uname -a; nslookup `hostname`; rpm -qa | grep  
Centrify*; adsec -support
```

For Solaris computers:

```
hostname ; uname -a; nslookup `hostname`; pkginfo -l  
CentrifyDS; adsec -support
```

For Debian computers:

```
hostname ; uname -a; nslookup `hostname`; dpkg -l | grep  
centrify*; adsec -support
```

Configuring a Linux server for DirectAccess

This chapter provides step-by-step instructions for how to control access to a Linux server with Centrify DirectSecure using Microsoft DirectAccess and the DirectAccess Test Lab environment.

The following topics are covered:

- [Introduction to Microsoft DirectAccess](#)
- [Sample configuration overview](#)
- [Step 1: Set up the DirectAccess test lab](#)
- [Step 2: Configure the LINX1 Linux server](#)
- [Step 3: Configure the DC1 domain controller](#)
- [Step 4: Verify IPv6 settings](#)
- [Step 5: Update group policies on LINX1 server](#)
- [Step 6: Start Apache Web Server](#)
- [Step 7: Update group policy settings for Client1](#)
- [Step 8: Verify DirectAccess functionality for Client1](#)

Introduction to Microsoft DirectAccess

DirectAccess is a technology introduced in the Windows 7 and Windows Server 2008 R2 operating systems that enables remote users to access Windows servers on corporate intranets without connecting to a virtual private network (VPN).

Centrify DirectSecure extends DirectAccess to enable secure access to Linux servers within a corporate intranet.

Microsoft provides extensive documentation and samples for DirectAccess, including the [Microsoft DirectAccess Test Lab Guide](#), which shows how to set up a simulated DirectAccess environment with Windows servers and client computers.

Centrify DirectSecure integrates seamlessly with Microsoft DirectAccess. The step-by-step instructions in this chapter demonstrate how to add a Linux server running Centrify DirectSecure to a DirectAccess-configured intranet and access the server's resources from a remote client computer through a DirectAccess connection.

Note The instructions in this chapter are only for the purpose of demonstrating Centrify DirectSecure functionality. The sample configuration does not reflect best practices nor does it serve as the basis for a DirectAccess production environment.

Sample configuration overview

You need the following computers to set up the sample DirectAccess environment:

- A Linux server named LINX1 that is running kernel 2.6.25 or later, and is configured as a general application server.
- A Windows Server 2008 R2 Enterprise Edition computer named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, Dynamic Host Configuration Protocol (DHCP) server, and an enterprise root certification authority (CA).
- A Windows Server 2008 R2 Enterprise Edition intranet member server named APP1 that is configured as a general application server and network location server.
- A Windows Server 2008 R2 Enterprise Edition intranet member server named EDGE1 that is configured as the DirectAccess server.
- A Windows Server 2008 R2 Enterprise Edition standalone server named INET1 that is configured as an Internet DNS server, DHCP server, and web server.
- A Windows 7 Ultimate Edition client computer named NAT1 that is configured to use a network address translator (NAT) device using Internet Connection Sharing.
- A Windows 7 Ultimate Edition roaming member client computer named CLIENT1 that is configured as a DirectAccess client.

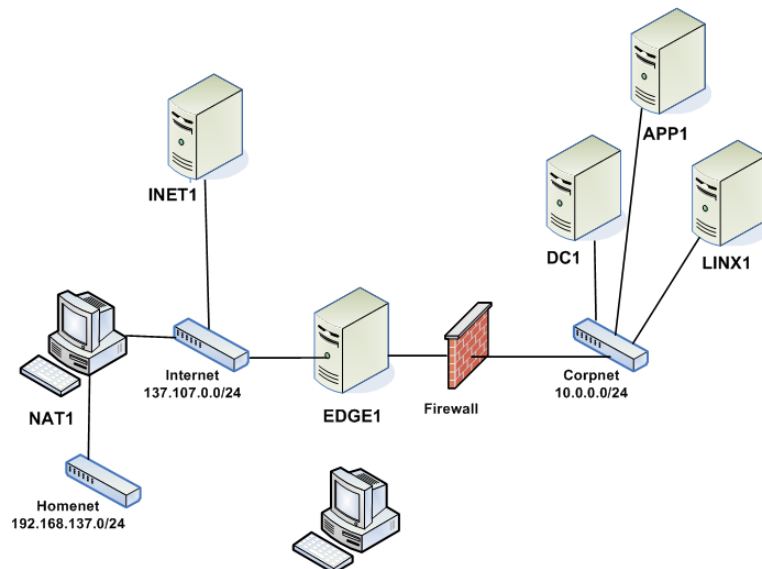
Note If you have already set up the [Microsoft DirectAccess Test Lab](#), LINX1 is the only computer that is new for setting up an environment

that includes DirectSecure. All of the Windows computers are part of the standard Test Lab configuration for Microsoft DirectAccess.

The DirectAccess test lab consists of three subnets that simulate the following:

- The Internet (131.107.0.0/24).
- A home network named Homenet (192.168.137.0/24) connected to the Internet by a NAT.
- An intranet named Corpnet (10.0.0.0/24) separated from the Internet by the DirectAccess server.

Computers on each subnet connect using a hub, switch, or virtual switch. See the following figure.



DirectAccess Resources

Microsoft provides extensive DirectAccess documentation, including the following:

- [Microsoft DirectAccess Solutions home page](#)—Provides links to specific Microsoft DirectAccess resources and documentation.
- [Microsoft Test Lab Guide for DirectAccess](#)—Provides step-by-step instructions for setting up the simulated DirectAccess environment that is the basis for the sample configuration in this chapter.

- **Troubleshoot DirectAccess**—A companion to the Test Lab Guide that provides tools and information for troubleshooting issues with DirectAccess.
- **Step 3: Configure the DC1 domain controller**
DC1 is already configured as a domain controller, as the DNS and DHCP server for the Corpnet subnet, and as the enterprise root CA for the domain; it is also configured for Windows DirectAccess.

Step 1: Set up the DirectAccess test lab

The starting point for the configuration in this chapter is the DirectAccess test lab.

The starting point for testing how to access a Linux server with Centrify DirectSecure through Microsoft DirectAccess is the Microsoft DirectAccess Test Lab. To set up the DirectAccess test lab, complete *all* the procedures *exactly* as described in the [Microsoft Test Lab Guide for DirectAccess](#).

When finished, you should have a working lab configuration with:

- Four servers and two client computers.
- A network with simulated home network, the Internet, and a corporate intranet

The test lab configuration with the added Linux server is illustrated in [“Sample configuration overview”](#) on page 44.

Step 2: Configure the LINX1 Linux server

To configure the Linux server, you must install the Centrify DirectControl agent, join the domain, and install Centrify DirectSecure.

To install the DirectControl agent on the LINX1 Linux computer:

- 1 Run the `install.sh` command to install the platform-specific Centrify DirectControl agent and optional packages. For example:

```
./install.sh
```

- 2 Follow the prompts displayed to select the tasks to perform and components to install.

You can accept the default that the installer provides for many of the prompts by pressing **Enter**.

For the zone, enter **NULL_AUTO**, which joins you to the domain through Auto Zone, a mechanism that Centrify DirectControl provides to join Active Directory without installing the DirectControl Console on DC1 and configuring a zone.

```
Do you want to run adcheck to verify your AD environment?:y
Join an Active Directory domain: Y
Enter the Active Directory domain to join: corp.contoso.com
Enter the Active Directory authorized user [administrator]
Enter the password for the Active Directory user:
Enter the computer name [LINX1]
Enter the container DN [Computers]
Enter the name of the zone [default]: NULL_AUTO
Enter the name of the domain controller [auto detect]
Reboot the computer after installation: Y
```

For more information about installation options, see the *Centrify Server Suite Planning and Deployment Guide*.

- 3 After verifying that the information in the installation summary is correct, type **Y** and press **Enter** to install the DirectControl agent and join the domain.
- 4 To verify the installation and that the DirectControl agent is running, open a terminal window and type the `adinfo` command, and you should see information similar to the following:

```
[root]# adinfo
...
Local host name:      linx1
Joined to domain:    corp.contoso.com
Joined as:           linx1.corp.contoso.com
Pre-win2kname:       linx1
Current DC:          dc1.corp.contoso.com
Preferred site:      Default-FirstSite-Name
Zone:                Auto Zone
CentrifyDC mode:     connected
Licensed Features:   Enabled
```

When you join the domain, a computer account is created for LINX1 in Active Directory.

To install Centrify DirectSecure on the LINX1 computer:

- 1 Copy the appropriate package for the local computer's operating environment to a local directory.

For example, if the operating environment is Red Hat Enterprise Linux:

```
cp /mnt/cdrom/Unix/centrify-ds-release-rhel4.6-i386.rpm .
```

If you aren't sure which file to use for the local operating environment, see the `release-notes` text file included in the package.

- 2 Run the appropriate command for installing the package based on the local computer's operating environment.

For example, for Red Hat Enterprise Linux, you can use:

```
rpm -ivh centrifyds-release-rhel4.6-i386.rpm
```

Step 3: Configure the DC1 domain controller

Configure the DC1 domain controller server as follows:

- Create a DirectAccess server security group
- Apply DirectAccess policies to Linux server

Create a DirectAccess server security group

You need to update the DirectAccess policies to apply to the LINX1 server. To facilitate this process, Centrify DirectSecure provides a script (see ["Apply DirectAccess policies to Linux server" on page 49](#)) that updates the required policies. The script applies the policies to a security group named `DA_Servers`, so before running the script, you need to create the group and add LINX1 to it.

To create the `DA_Servers` group:

- 1 In the Active Directory Users and Computers console tree, right-click **Users**, then click **New > Group**.
- 2 In the dialog box, under **Group name**, type **DA_Servers**.

- 3 Under **Group scope**, choose **Global**; under **Group type**, choose **Security**; then click **OK**.
- 4 In the details pane, double-click **DA_Servers**.
- 5 In the **DA_Clients Properties** dialog box, click the **Members** tab, and then click **Add**.
- 6 In the **Select Users, Contacts, Computers, or Groups** dialog box, click **Object Types**, click **Computers**, and then click **OK**.
- 7 Under **Enter the object names to select (examples)**, type **LINX1**, and then click **OK**.
- 8 Verify that **LINX1** is displayed below **Members**, and then click **OK**.

Apply DirectAccess policies to Linux server

Centrify DirectSecure provides a PowerShell script to apply DirectAccess policies to the LINX1 Linux server (actually, to the DA_Servers security group, which includes the LINX1 server). For more information, see [“Create a DirectAccess server security group” on page 48](#).

The script is available from the [Centrify Download Center](#).

To run the script:

- 1 Copy the script, `damod.ps1`, from the [Centrify Download Center](#) to a location on DC1.
- 2 Open a **PowerShell** window, for example:
Start > All Programs > Accessories > Windows PowerShell
- 3 Enable scripting by typing the following command:
`set-executionpolicy remotesigned`
- 4 The script uses the `get-gpo` cmdlet, which may not be available; to make it available, type the following command:
`import-module grouppolicy`
- 5 Change to the directory containing the script, then type:
`.\damod.ps1`

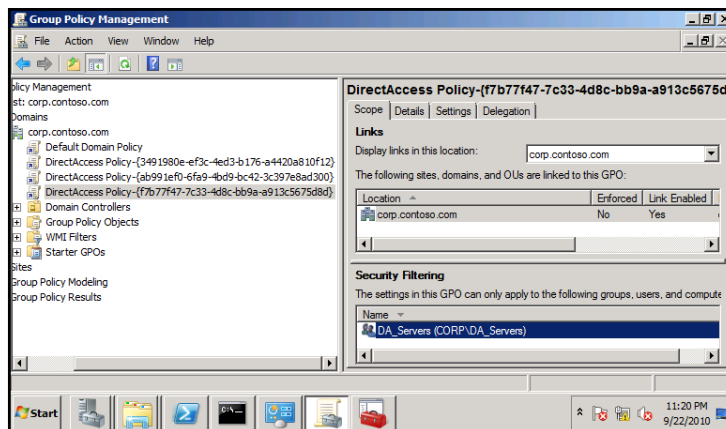
The script creates a DirectAccess policy and applies it to the DA_Servers group.

Assign the group policy

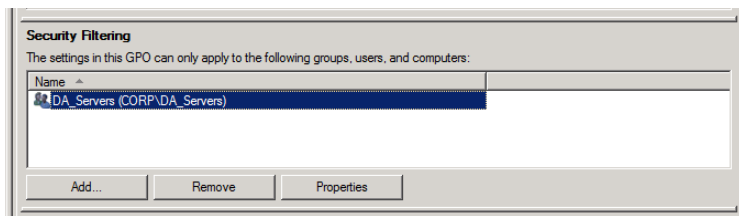
You need to assign the policy to make it active.

To assign the policy:

- 1 Open the Group Policy Editor.
- 2 Expand **Domains > corpnet**.
- 3 You should see three DirectAccess policies under this node:



- 4 Scroll to the third one, right-click, and click **Edit**. The policy created by the script applies to the DA_Servers group, so you should see **DA_Servers** listed in **Security Filtering**; if not, open one of the other policies and verify that it is the policy that applies to **DA_Servers**.



- 5 In the console tree, expand **Computer Configuration > Policies > Windows Settings > Security Settings > IP Security Policies on Active Directory**.

- 6 In the details pane, select **DA**, then right-click and click **Assign**.

Step 4: Verify IPv6 settings

Verify that IPv6 configuration is enabled for the network interfaces on LINX1.

After you update group policies, DirectSecure will automatically create an ISATAP adapter for LINX1.

Step 5: Update group policies on LINX1 server

Now update group policies to apply the DirectAccess policies to LINX1.

To update group policies:

- 1 Open a terminal window.
- 2 Run the following command:
- 3 To verify that the DirectAccess policies have been applied to the LINX1 server, run the following DirectSecure command, and you should see similar results:

```
adgpupdate
```

```
[root]# adsec
...
GP Management of IPsec is enabled
IKE service ... running
```

Step 6: Start Apache Web Server

You need to start the Apache Web Server so you can verify DirectAccess connectivity.

To start the Apache Web Server:

- 1 Open a terminal window.
- 2 Run the following command:

```
[root]# service httpd start
```

Step 7: Update group policy settings for Client1

You need to update group policy settings for the Client1 computer.

To update group policy settings on Client1:

- 1 Open a **Command Prompt** window.
- 2 Type:
`gpupdate`

Step 8: Verify DirectAccess functionality for Client1

After you update group policy settings for the Client1 computer, verify that it can access resources on the LINX1 server that has been added to the DirectAccess configuration.

To verify that Client1 has access to LINX1 resources with intranet connectivity:

- 1 Unplug the Ethernet cable of CLIENT1 from the switch for the Homenet subnet and plug it into the switch for the Corpnet subnet.
- 2 Log on to Client1 by using the User1 account.

Open Internet Explorer. In the Address bar of Internet Explorer, type **<http://linx1.corp.contoso.com/>**, press **ENTER**, and then press **F5**. You should see the default page for the Apache Web Server.

Configuring a Certificate Authority for auto-enrollment

This section describes how to set up a Certificate Authority with the Microsoft Windows **certificate auto-enrollment feature** to support PKI authentication for Centrify DirectSecure.

The following topics are covered:

- Working with a single Certificate Authority for UNIX
- Preparing a computer to be a Certificate Authority (CA)
- Adding a trusted root certificate to the group policy
- Enabling auto-enrollment
- Creating a certificate template with auto-enrollment permission
- Assigning the certificate template to the CA
- Understanding how DirectSecure updates CRLs

Working with a single Certificate Authority for UNIX

Centrify DirectSecure relies on the Microsoft Windows public key infrastructure (PKI) to obtain the certificates for the UNIX computers that are joined to a domain. The most basic configuration of the Windows PKI environment provides a Windows server as the Certificate Authority (CA) that issues and manages security credentials and public keys through the exchange of encrypted digital certificates. DirectSecure then uses the Microsoft Windows **certificate auto-enrollment feature** of the Certificate Authority to make certificates available to UNIX computers.

This section describes how to set up a basic environment that has a single, enterprise root Certificate Authority (CA). In this scenario, the Certificate Authority is a Microsoft Enterprise Certificate Server that issues all certificates. In a production environment, you may have more complex requirements that include multiple CAs configured for a

domain. However, setting up this sample environment should give you enough information to extend your PKI configuration to a more complex environment.

Note Centrify DirectSecure requires a Microsoft Windows Server to be configured as the Certification Authority (CA) for the Active Directory forest. Other Certification Authority certificate issuers are not currently supported.

Preparing a computer to be a Certificate Authority (CA)

The first step in configuring the environment is to identify a computer to be the Certificate Authority server for the Active Directory forest. In most cases, the computer should be an Active Directory domain controller. To become a Certificate Authority, the computer also requires Microsoft Internet Information Services (IIS) and Certificate Services to be installed.

Microsoft Internet Information Services (IIS) are required to handle Certificate Revocation List (CRL) requests made by DirectSecure and to provide the virtual directories required to issue and manage certificates.

Certificate Services are required to enable the computer to act as a Certificate Authority (CA) and issue certificates to other computers that join the domain. The Application server role, which installs IIS, and the Certificate Services server role must be on the same computer. Therefore Centrify recommends that you install IIS at the same time you install Certificate Services.

What's required to install Certificate Services

Before installing Certificate Services, check that you have the following:

- Account credentials for an account that is an Enterprise Administrator or a Domain Administrator of the forest root domain of the Active Directory forest.
- A computer with Windows Server 2008 Enterprise Edition, or later, operating system. Previous versions of Windows Server do not

support auto-enrollment within the certificate templates. In addition, the computer must be running Enterprise Edition because Standard Edition does not support the V2 or V3 certificate templates that are required for auto-enrollment.

- Active Directory services must be installed on the Certificate Services server. If you install the Certificate Services server role on a domain controller, no further action is required. When you promote a computer to be a domain controller, the Active Directory services are installed automatically.

Add the required server roles to make the computer a Certificate Authority

After you have verified you have an appropriate account and computer, you can use the Control Panel to add the appropriate server roles.

To install IIS and Certificate Services on a Windows Server:

- 1 Open the wizard that enables you to manage roles and features.
For example, on a Windows 2008 computer, open Server Manager and click **Add Roles**. In the Add Roles Wizard window, click **Server Roles**.
- 2 Select **Active Directory Certificate Services** and **Application Server (IIS)**, then click **Add Required Role Services** in the pop-up window.
- 3 Click **Next** to accept the default values.
For the type of the computer be certain to choose **Enterprise**, then **Root CA**.
- 4 Enter a name for the CA, then click **Next** to accept the default values on each screen.
- 5 Click **Finish** to complete installation.

After you have added the server roles and created the CA, you can view the CA you just created by using the MMC Certification Authority snap-in.

Adding a trusted root certificate to the group policy

To establish a chain of trust for your PKI environment, you identify the CA you just created as a trust anchor.

To establish the CA as a trust anchor, add the root certificate for the CA to the **Trusted Root Certification Authorities** container in the group policy object that defines the IP Security policies.

To add a trusted root certificate to the group policy object:

- 1 Open the Certificates (MMC) snap-in.
If the Certificates snap-in is not available, you can run MMC and click **File > Add/Remove Snap-in** to add it.
- 2 Click **Certificates > Trusted Root Certification Authorities > Certificates**.
- 3 Select the root certificate generated by the CA you created in the previous procedure, then double-click it to see its Properties page.
- 4 Click the **Details** tab; then click **Copy to file** to start the Certificate Export Wizard. In the wizard, make the following selections:
 - **File format:** *DER encoded binary X.509 (.CER)*
 - **File Name:** Anywhere on the local server
 - **Include all certificates in the certification path:** *No*
- 5 Open the Group Policy Object Editor and select the group policy object that defines the IP Security policies.
- 6 Click **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies > Trusted Root Certification Authorities**.
- 7 Select **Trusted Root Certification Authorities**, right click, and select **Import** to open the Certificate Import Wizard.
- 8 Click **Next** on the Welcome screen.

- 9 Browse to find the root certificate you copied in **Step 4**, then click to accept the default values on each screen.
- 10 Click **Finish** to complete the wizard.

The root certificate is now in the Active Directory Trusted Root Certification Authorities container. Certificates in this container are downloaded to any computer that joins the domain to establish trust for the root CA.

Enabling auto-enrollment

Centrify DirectSecure uses the Microsoft Windows **certificate auto-enrollment feature** to make certificates available to UNIX computers. If auto-enrollment is enabled, when a UNIX computer joins a domain, DirectSecure requests certificates from the CA based on particular templates, and installs them on the joined computer.

To enable auto-enrollment, you must do the following:

- Enable auto-enrollment for the group policy.
- Create a certificate template with auto-enrollment enabled.

Enabling auto-enrollment for the group policy

To enable auto-enrollment for the group policy:

- 1 Open the Group Policy Object Editor and select the group policy object that defines IPsec policies.
- 2 In the left pane, click **Computer Configuration > Policies > Windows Settings > Security Settings > Public Key Policies**.
- 3 In the right pane, right-click **Certificate Services Client - Auto - Enrollment**, then select **Properties** to open the Auto-Enrollment Settings Properties page.
- 4 Make sure that **Enabled** is selected for Configuration Model and check the following boxes:
 - **Renew expired certificate, update pending certificates, and remove revoked certificates.**

- **Update certificates that use certificate templates.**

5 Click **OK** to save the auto-enrollment settings.

Creating a certificate template with auto-enrollment permission

DirectSecure supports certificate templates that use RSA or Elliptic Curve Cryptography (ECC) algorithms. For details about using the ECC algorithm, see [“Using the ECC algorithm in a certificate template” on page 58](#).

To configure a template with auto-enrollment:

1 Open the MMC Certificate Template snap-in.

Another way to open the Certificate Template console is to open the Certificate Authority console, select **Certificate Templates**, then right-click and select **Manage**.

2 Select a template, then right-click and select **Duplicate Template** to create a new template that you can modify.

For example, select the Workstation Authentication template.

3 On the Properties page for the new template, do the following:

- a Select the **General** tab and enter a name for the template.
- b Select the **Security** tab and select **Domain Computers**. Then select **Read** and **Autoenroll** permissions.
- c Select the **Extensions** tab. Then select **Application Policies**.
- d Click **Edit**. **Client Authentication** should already be shown.
- e Click **Add**, then scroll and select **Server Authentication**.
- f Click **OK**.

4 Click **OK** to save the new template.

Using the ECC algorithm in a certificate template

If you wish to use the ECC algorithm in your certificate template, be aware of the following points:

- Older versions of Windows do not support the ECC algorithm. When you create the certificate template, be sure to set the compatibility settings for both the CA and the certificate recipient to Windows Server 2008 or newer.
- You specify the ECC algorithm on the Cryptography tab, with the following settings:
 - Provider category: Key Storage Provider
 - Algorithm name: Select either ECDH_P256, ECDH_P384, or ECDH_P521.

Assigning the certificate template to the CA

You can now assign the newly created template to the Certificate Authority. Whenever a computer joins the domain, the CA issues a certificate based on the template, and Centrify DirectSecure downloads the certificate to the computer.

To assign the template to a certificate authority (CA):

- 1 Open the Certification Authority console.
- 2 Click **Certification Authority** > *CA_name* > **Certificate Templates**, where *CA_name* is the container for the CA you set up earlier. See [“Preparing a computer to be a Certificate Authority \(CA\)” on page 54](#).
- 3 Right-click and select **New** > **Certificate Template to Issue**. Select the template you just created and click **OK**.

The root CA is now set up to issue certificates based on the template you created.

Understanding how DirectSecure updates CRLs

Generating a certificate revocation list (CRL) is the method a Certificate Authority (CA) uses to maintain the validity of the certificates that it issues. A CRL contains a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked or are no longer valid, and therefore should not be relied upon. DirectSecure

retrieves CRLs from CAs after specific events (such as joining a domain) and at specific intervals to determine which certificates, if any, have been revoked, and thus whether to request new certificates.

Note The current version of DirectSecure only supports complete certificate lists, not delta CRLs, which only describe the updates since the complete list was published.

Generating a CRL

A CRL is generated by a CA and contains a list of certificates to revoke from the list of certificates that the CA has issued.

Typically, a CA automatically generates a CRL at a specified interval, anywhere from two hours to one year, at which point the new CRL with the list of revoked certificates is available for clients to request.

The CRL itself contains the interval period, which allows clients, such as DirectSecure, to determine when to request a new CRL. See [“Retrieving a CRL and verifying certificates” on page 60](#) for information about retrieving CRLs.

In addition to automatic generation of a CRL, Active Directory utilities are available that allow an administrator to manually revoke certificates and publish a CRL on the CA. In this case, the CRL-publishing interval is reset so the next automatic publishing operation will occur in the appropriate amount of time.

Retrieving a CRL and verifying certificates

At specific times (when the UNIX system joins a domain, the administrator issues the `adgpupdate` command, or the group policy refresh interval occurs), DirectSecure performs certain tasks, including determining whether to retrieve a CRL. Specifically, DirectSecure does the following:

- Identifies the CA that issued certificates for the system.
- Looks at the refresh interval in the current CRL to determine whether to retrieve a new CRL.
- If the interval has expired, retrieves a new CRL by using the IIS Web Server for the CA.

- Verifies the currently issued certificates against the CRL and requests new certificates for certificates that have been revoked.

Note When you manually revoke a certificate, it is possible that the certificate will appear as valid even after running the `adgpupdate` command to trigger an IPsec update. When you revoke a certificate, DirectSecure first looks at the current CRL to determine the validity of the certificates that have been issued. In this case, the newly revoked certificate still appears as valid. Immediately afterwards, because of the IPsec update, DirectSecure requests a new CRL. The new CRL shows that the certificate in question is invalid, but DirectSecure will not look at the new CRL until the next scheduled update, or until you run the `adgpupdate` command again. Therefore, to be certain to have current information, if you manually revoke certificates, you can issue the `adgpupdate` command twice in sequence.

Index

A

- Accept unsecured communication 38
- Activate default response rule 32
- adsec
 - command syntax 26
 - examples 29
 - options 27
 - policies applied 24
 - verifying IKE service status 20
 - warnings 31
- AH and ESP mixing warning 37
- authentication
 - about 11
 - Kerberos 11
 - pre-shared keys 11

C

- Centrify DirectControl
 - Test Lab configuration 46
- Centrify website 7
- Certificate Authority (CA)
 - generating certificate revocation lists 59
 - infrastructure requirements 17
 - requirements 54
- Certificate Services
 - adding Windows components 55
 - operating system requirements 17
 - requirements 54
- certificate templates 13
- Client1
 - verify connection 52
- conventions, documentation 6

D

- damod.ps1 script 49
- data and address integrity (AH) 37
- data integrity and encryption (ESP) 37
- destination address warning 34

Diffie-Hellman group 33

DirectAccess

- configuration overview 44 to 45
- extending Test Lab 43
- introduction to 43
- PowerShell script 49
- security group 48
- updating group policies 51
- verifying Linux access 52

DirectAccess Test Lab

- set up 46

DirectSecure

- basic architecture 9
- install for test lab 48
- previously configured environment 16
- retrieving a certificate revocation list 60
- UNIX platforms 18
- unsupported features 25
- Windows platforms 17

documentation

- additional 7
- audience 5
- conventions 6
- summary of contents 5 to 6

domain controller

- Active Directory services 12
- encrypting traffic to 15, 21
- operating system requirements 17
- Test Lab configuration 48
- using for Certificate Services 54

E

ESP and AH mixing warning 37

F

ftp failure 26

I

installation

- DirectSecure package 18, 48



- native or package management programs
18
- Internet Information Services (IIS)
 - Application server role 54
 - installing 55
 - requirement 12, 54
- Internet Key Exchange (IKE) 9
- IP Security
 - configuring for Windows computers 16, 17
 - introduction 8
 - key lifetime setting 35
 - unsupported features 25
- K**
- Kerberos authentication 11
- key lifetimes 35
- L**
- Linux server
 - naming convention 6
 - set up 46 to 48
 - update group policies 51
- LINX1. See Linux server
- M**
- Microsoft
 - Certificate Authority (CA) requirement 12, 54
 - Certificate Services 13, 54
 - DirectAccess Test Lab Guide 43
 - Internet Information Services (IIS) 13, 54
- Mixing ESP and AH 37
- MS default rules are not supported 32
- O**
- open ports 23
- P**
- ping failure 26
- port, TCP requirement 23
- PowerShell script 49
- pre-shared key authentication 11
- public key infrastructure (PKI)
 - about 11 to 14
 - account credentials 54
 - assigning a certificate template 59
 - auto-enrollment 57
 - services and server roles 54
 - single Certificate Authority 53
 - trusted root certificate 56
- R**
- Red Hat Enterprise Linux
 - installation command 19
 - software package name 18
- root user
 - installation requirement 18
 - shared key protection 11
- S**
- security associations (SA) 26
- server roles 55
- T**
- Test Lab. See DirectAccess Test Lab
- U**
- UNIX
 - adsec command-line 26
 - naming convention 6
 - supported platforms 18
- unsecured communication settings 38
- unsupported features 25
- W**
- warnings
 - changing policy action 39
 - default rules are not supported 32
 - destination address not supported 34
 - Diffie-Hellman group 33
 - Lifetime (secs) 36
 - mixing ESP and AH 37
- Windows
 - Certificate Authority (CA) requirement 12
 - having a working environment 16
 - operating system requirements 54



supported platforms 17