

Centrify for Apache 5.5.2 Release Notes

© 2004-2019 Centrify Corporation.

This software is protected by international copyright laws.

All Rights Reserved.

Table of Contents

1.	About This Release.....	1
2.	Package Contents.....	2
3.	Supported Platforms.....	2
4.	Feature Changes	3
4.1.	Feature Changes in Centrify for Apache 5.5.2 (Release 18.11)	3
5.	Bugs Fixed	3
5.1.	Bug Fixed in Centrify for Apache 5.5.2 (Release 18.11).....	3
6.	Getting Started	3
7.	Known Issues	3
7.1.	Known issues on All	3
7.2.	Known issues on AIX	6
7.3.	Known issues on HPUX	6
7.4.	Known issues on Solaris.....	7
7.5.	Known issues on RHEL	7
8.	Additional Information and Support.....	8

1. About This Release

Centrify Authentication Service provides secure access control and centralized identity management by seamlessly integrating UNIX and Linux computers with Microsoft Active Directory.

Centrify for Apache extends Centrify Authentication Service to Apache HTTP servers. This solution allows you to use Microsoft Active Directory as the centralized authentication and access control data store in a heterogeneous environment containing Windows and UNIX computers, as well as Apache HTTP servers.

Documentation, Authentication Guide for Apache Servers (centrify-apache-guide.pdf), is available online to guide customers through the setup and configuration of Centrify for Apache in both new and existing environments.

The latest copies of this release notes as well as the above-mentioned documentation are available online at <http://docs.centrify.com>.

Centrify software is protected by U.S. Patents 7,591,005; 8,024,360; 8,321,523; 9,015,103; 9,112,846; 9,197,670; 9,378,391 and 9,442,962. (Ref: CS-44575)

2. Package Contents

The Centrify for Apache bundle package contains the following resources:

- Centrify for Apache software package (e.g. rpm, or deb file)
- Centrify for Apache Release Notes (Centrify-for-Apache-Release-Notes.html - this release notes)

3. Supported Platforms

The Centrify for Apache bundle package is available on the following OS/platforms in this release:

- Debian Linux on x86_64
- HP-UX on Itanium
- HP-UX on PA-RISC
- IBM AIX on PPC
- Oracle Solaris on SPARC
- Oracle Solaris on x86_64
- Red Hat Enterprise Linux on x86_64
- Red Hat Fedora Linux on x86_64
- SUSE Linux Enterprise Server on x86_64
- Ubuntu Server on x86_64

This release supports Apache HTTP Server v2.4.

For the OS versions that a Centrify for Apache bundle package supports, please refer to the supported OS versions of the matching DirectControl agent package in the corresponding Centrify Authentication Service release. Similarly, Centrify for Apache also follows Centrify DirectControl's schedule for End-of-Support platforms and hence please refer to the announcements there.

4. Feature Changes

4.1. Feature Changes in Centrify for Apache 5.5.2 (Release 18.11)

This release of Centrify for Apache works with Centrify Infrastructure Services Release 18.11.

Note: This product, Centrify for Apache, is already deprecated. The release 5.5.2 is the last release in the form of just a "refresh" release for existing customers only and we are going to support it for only one more year. (Ref: CS-47663)

5. Bugs Fixed

5.1. Bug Fixed in Centrify for Apache 5.5.2 (Release 18.11)

This release fixed the issues that the package bundled some unnecessary libraries like libcrypto.so, and unnecessarily emitted "provides" messages. (Ref: CS-47665)

6. Getting Started

First read the `centrify-apache-guide.pdf` to get familiar with how to use this feature, and the installation, upgrade, configuration and verification procedures.

7. Known Issues

The following sections describe common known issues or limitations associated with this release.

7.1. Known issues on All

- NTLM does not work for users in a disjoint AD domain

If you have a disjoint domain and have not configured the browser to use silent authentication, use the NETBIOS name (for example MYDOMAIN\username) for NTLM authentication. The full name (for example username@mydomain.com) does not work. If you have configured your browser for silent authentication, the browser automatically uses the NETBIOS name.

- Basic authentication fails using pre-Windows 2000 name

Basic authentication using the domain\username format is not supported in this release. If you need to use basic authentication you should use the username@domain.com format.

- Custom user LDAP attributes and LDAP attribute caching

Only string values are supported at this time. For LDAP attributes with multiple values, only the first value is set in an environment variable or HTTP header. If an attribute with a binary value is set in CustomAttributes, the resulting format of the value string in the environment variable or HTTP header is undefined.

For the CustomAttributes directive, only some LDAP attributes are cached by the adclient daemon in DirectControl. LDAP attributes that are not cached by adclient are fetched from the AD on each request. The user LDAP attributes cached by adclient in DirectControl are:

- objectCategory
- objectClass
- displayName
- cn
- uSNChanged
- sIDHistory
- sAMAccountName
- name
- primaryGroupID
- userPrincipalName
- servicePrincipalName
- userWorkstations
- userAccountControl
- lockoutTime
- pwdLastSet
- accountExpires
- logonHours
- msDS-KeyVersionNumber
- homeDirectory
- homeDrive
- altSecurityIdentities
- gecos
- mail
- department
- description
- mobile
- title
- telephoneNumber
- unixUserPassword
- msSFU30Password

- NTLM v1 authentication issues

When performing NTLM authentication manually (non-silently) through a pop-up dialog, authentication with an incorrect domain in a NetBIOS name, for example, BADDOMAIN\jillsmith, may still authenticate successfully as, for example, jillsmith@mydomain.com, where mydomain.com is the AD domain that the machine is joined to.

Entering a bad domain in UPN format, for example, jillsmith@baddomain.com does not have this problem, i.e. will not authenticate successfully.

Also, when performing NTLM authentication manually (non-silently) through a pop-up dialog, authentication for a username in a child domain, for example, "jillsmith@childdomain.mydomain.com", will succeed but the authenticated username will have the parent domain, for example, jillsmith@mydomain.com, instead of the child domain, for example, jillsmith@childdomain.mydomain.com, where mydomain.com is the AD domain that the machine is joined to.

- Working with users from a one-way trusted forest with NTLM

To authenticate users from a one-way trusted forest using NTLM you must first specify the Active Directory to NTLM domain name mappings in

```
/etc/centrifydc/centrifydc.conf
```

file and restart adclient. See

```
/etc/centrifydc/centrifydc.conf
```

and look for "adclient.ntlm.domain" for more information.

In addition, the user's group information will be unavailable. This may be fixed in a future version of DirectControl.

- ADFS sample shows "(Unknown)"

After authenticating with ADFS to a Centrify ADFS sample, the resulting page shows

```
Your Identity is "username@domain.com". (Unknown)
```

Or the IDENTITY_TYPE environment variable or HTTP_IDENTITY_TYPE header value is "Unknown" in your Apache ADFS application. To workaround this, on the ADFS server:

1. Add a claim rule for the application using the

```
Send LDAP Attribute as Claims
```

```
template, and set the "LDAP Attribute" to "User-Principal-Name" and the "Outgoing Claim Type" to "AD FS 1.x UPN".
```

2. Add a claim rule for the application using the

```
Transform an Incoming Claim
```

```
template, and set the "Incoming claim type" to "AD FS 1.x UPN", "Outgoing claim type" to "Name ID", and the "Outgoing nameID format" to "UPN"
```

- Using IP address to access ADFS sample

When using an IP address for the hostname when accessing a Centrify Apache ADFS sample, the following error results:

```
Error
adfsserver.resourcedomain.com
```

There was a problem accessing the site. Try to browse to the site again.

If the problem persists, contact the administrator of this site and provide the reference number to identify the problem.

Reference number: 04b9c156-4753-4393-a71b-86b84fdd1bb8

To work around this, use the IP address in the application's EntryUrl directive in the Apache configuration file, as well as in the

```
Application URL
```

property for the application on ADFS 1.0 server, or in the

```
Relying party identifier
```

property for the application on ADFS 2.0 server.

7.2. Known issues on AIX

- Loading the Centrify DirectControl modules in the proper order

In this release, the mod_auth_centrify module needs to be dynamically loaded before the mod_adfs_centrify module. Therefore, if you are modifying the Apache server configuration file to load these modules, you must specify:

```
LoadModule centrifydc_auth_module
/usr/share/centrifydc/apache/lib/mod_auth_centrifydc_xx.so
```

before specifying:

```
LoadModule centrifydc_adfs_module
/usr/share/centrifydc/apache/lib/mod_adfs_centrifydc_xx.so
```

7.3. Known issues on HPUX

- Loading the Centrify DirectControl modules in the proper order

In this release, the mod_auth_centrify module needs to be dynamically loaded before the mod_adfs_centrify module. Therefore,

if you are modifying the Apache server configuration file to load these modules, you must specify:

```
LoadModule centrifydc_auth_module
/usr/share/centrifydc/apache/lib/mod_auth_centrifydc_xx.so
```

before specifying:

```
LoadModule centrifydc_adfs_module
/usr/share/centrifydc/apache/lib/mod_adfs_centrifydc_xx.so
```

- NTLM authentication causes internal server errors

When users enter domain names while using NTLM authentication, incorrect domain names may cause this effect. If you are using Apache on HP-UX, you may want to increase the `adclient.dns.response.maxtime` parameter in:

```
/etc/centrifydc/centrifydc.conf
```

the DirectControl configuration file, to avoid issues when users mistype domain names.

- PAM authentication is not supported

In the "Require" directive, the PAM authentication is not supported. This version only supports logging in using the Active Directory credentials.

7.4. Known issues on Solaris

- Loading the Centrify DirectControl modules in the proper order

In this release, the `mod_auth_centrify` module needs to be dynamically loaded before the `mod_adfs_centrify` module. Therefore, if you are modifying the Apache server configuration file to load these modules, you must specify:

```
LoadModule centrifydc_auth_module
/usr/share/centrifydc/apache/lib/mod_auth_centrifydc_xx.so
```

before specifying:

```
LoadModule centrifydc_adfs_module
/usr/share/centrifydc/apache/lib/mod_adfs_centrifydc_xx.so
```

7.5. Known issues on RHEL

- Adding Kerberos libraries to your search path

Fedora uses a version of the Apache server that loads Kerberos from the `/usr/lib` directory before loading the Centrify DirectControl

for Apache module. This causes a problem when the Centrify DirectControl for Apache module loads because it only has access to the standard Kerberos libraries, but the module requires Kerberos extensions that aren't in the standard Kerberos libraries.

To prevent this problem on computers running Fedora Core, you should add `/usr/share/centrifydc/kerberos/lib` to your library search path:

- 1 Create `/etc/ld.so.conf.d/centrify.conf` with the line `/usr/share/centrifydc/kerberos/lib`.
- 2 Run `ldconfig`.

8. Additional Information and Support

In addition to the documentation provided for this product, you can find the answers to common questions and information about any general or platform-specific known limitations as well as tips and suggestions from the Centrify Knowledge Base.

The Centrify Resources web site provides access to a wide range of information including analyst report, best practice brief, case study, datasheet, ebook, white papers, etc., that may help you optimize your use of Centrify products. For more information, see the Centrify Resources web site:

www.centrify.com/resources

You can also contact Centrify Support directly with your questions through the Centrify Web site, by email, or by telephone. To contact Centrify Support or to get help with installing or using this version of Centrify for Apache, send email to support@centrify.com or call 1-669-444-5200, option 2. For information about purchasing or evaluating Centrify products, send email to info@centrify.com.