

DEPLOYMENT GUIDE

Fortinet Security and Centrify



Fortinet Security and Centrify

Overview	3
Deployment Prerequisites	3
Architecture Overview	3
Figure 1: Topology.	3
Partner Configuration.	4
Centrify Cloud.	4
Figure 2: Connector Download	4
Figure 3: Connector Login	4
Figure 4: Connectors Configured	5
Figure 5: Adding Users.	5
Figure 6: Adding Roles	5
Fortinet Configuration	6
FortiGate RADIUS Authentication	6
Mobile Device Configuration	6
Dashboard and Reporting	6
Figure 7: Dashboard	6
Figure 8: User	6
Figure 9: Apps.	7
Figure 10: Endpoints.	7
Summary	7
Access to Centrify Demo	7
How to Get Help	7



Overview

Fortinet network security appliances and subscription services provide broad, integrated, and high-performance protection against dynamic security threats while simplifying the IT security infrastructure. Fortinet offers a flexible, end-to-end solution that incorporates

wireless and wired access, security, authentication, switching, and management in an easily managed system that allows systemwide policy enforcement. Centrify offers secure, single sign-on for cloud and mobile applications, as well as management of a broad variety of mobile devices, enabling enterprises to uniformly and efficiently manage identity and access policies for cloud and mobile resources combined with Fortinet's enterprise security. This provides the customer with the combined benefits of both on-premises and cloud-based unified identity services and enterprise security.

Architecture Overview

The following diagram illustrates the various services and components that are part of the Fortinet Centrify integration. Some of these Centrify services are delivered in the Centrify Cloud. This includes a FortiGate appliance and the Centrify Identity Platform, which provide the underlying infrastructure for the Centrify Identity Service and the Centrify Privilege Service. These cloud services are hosted on the Microsoft Azure Platform-as-a-Service and operated by Centrify.

Centrify also offers solutions such as Centrify Server Suite, which runs as a set of on-premises software services that provide direct integration with Microsoft Active Directory or LDAP directory services. The Centrify Cloud Connector acts as a secure connection between various on-premises services and the Centrify Cloud Services. Centrify, along with Fortinet, can provide secure identity management services across both on-premises platforms and mobile devices.

The Identity Platform can be used with existing Active Directory, LDAP infrastructures, or use Centrify's cloud-based directory or both.

Deployment Prerequisites

The Fortinet and Centrify deployment requires the following:

1. FortiGate Firewall
2. Network AD Server
3. Client Device connecting to the network
4. Centrify Software or Cloud Account

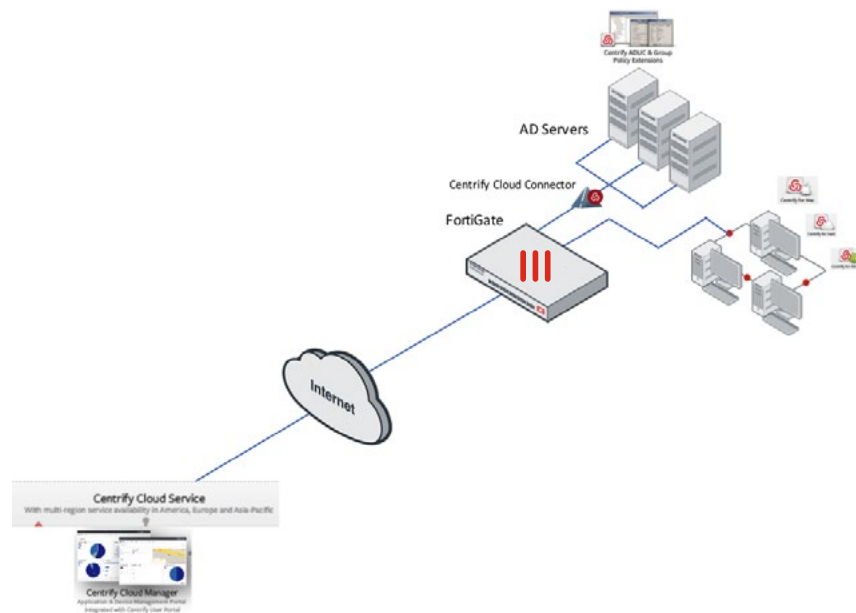


Figure 1: Topology

Partner Configuration

Centrifify Cloud

For customers who want to integrate the Centrifify Cloud with their on-premises Active Directory or LDAP directory for user authentication, the Centrifify-supplied software program called the Centrifify Cloud Connector needs to be installed inside their environment. The Centrifify Cloud Connector is a simple Windows service that runs behind a customer's firewall to provide real-time authentication, policy, and access to user profiles without synchronizing data to the cloud.

The Cloud Connector seamlessly integrates with Active Directory or LDAP without opening extra ports in an organization's firewall or adding devices in their DMZ, and it acts as a gateway for access to on-premises applications without the need for VPN.

When the Cloud Connector starts up, it creates a persistent, outbound connection over port 443 (https) to connect to the Azure cloud via the Microsoft Service Bus API. Traffic is encrypted and mutually authenticated (a "secure channel") between the Cloud Connector and the cloud tenant.

First complete registration with Centrifify. Log in to Centrifify and download the Cloud Connector. Steps to installing Centrifify Cloud Connector:

1. Log on to the Centrifify Cloud Manager at <http://cloud.centrifify.com/manage>.
2. Click on Settings → Network.
3. Click on Add Centrifify Connector.
4. Click Download and install it on your Windows AD server. See Figure 2.
5. Use Portal Credentials for user with "Register Proxies" rights to integrate your Active Directory with Centrifify Cloud Services. See Figure 3.

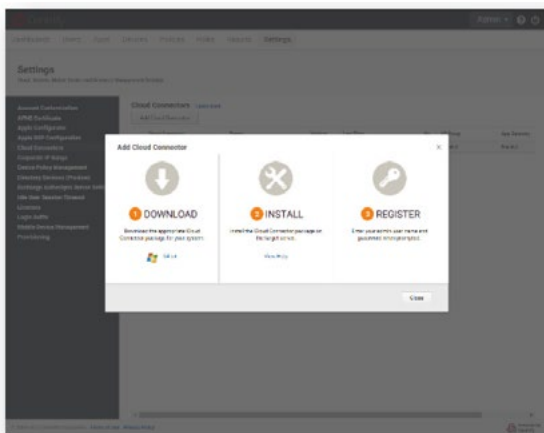


Figure 2: Connectors Download.

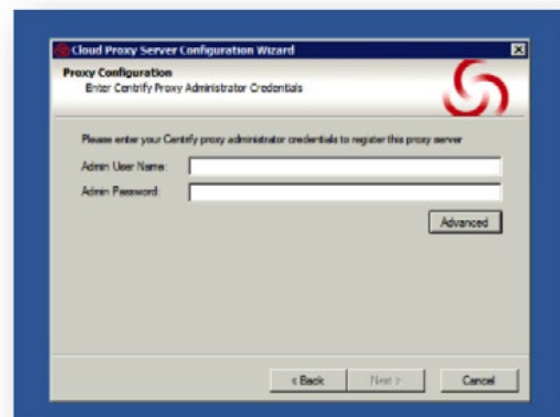


Figure 3: Connector Login.

On the Centrif Admin Portal, you should be able to see your server integrated and the status as active. This can be visible under Settings > Centrif Connectors. See Figure 4 below.

Centrif Connectors
Use these settings to add and manage connectors.
[Learn more](#)
Add Centrif Connector

Name	Forest	Version	Last Ping	Hostname	Enabled Services	Status
<input type="checkbox"/> WinServer2012	corp.fortidemo.com	17.1.151	02/23/2017 05:39 PM	WinServer2012	AD Proxy App Gateway LDAP Proxy RADIUS Server Web Server (WIA)	Inactive
<input type="checkbox"/> WIN-L2LOMJH04GN	corp.EntLabHW.local	17.5.152	06/06/2017 10:41 AM	WIN-L2LOMJH04GN	AD Proxy App Gateway LDAP Proxy RADIUS Server Web Server (WIA)	Active

Figure 4: Connectors Configured

The next step is to add Users. Click Core Services > User and Add User. You can also bulk import users. Figure 5 below shows how to import users from the AD server.

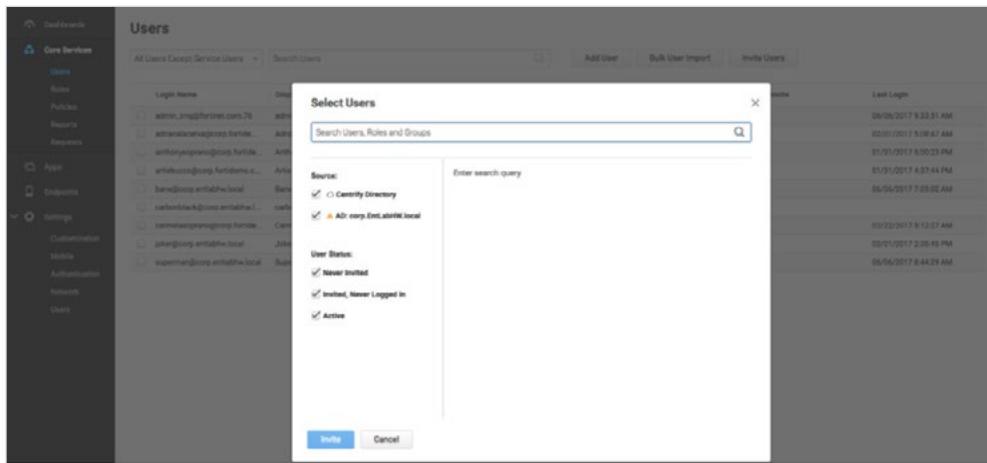


Figure 5: Adding Users.

You can also import the roles from the AD server or manually create roles as shown below.

Roles
Search roles Add Role

Name	Description
<input type="checkbox"/> Everybody	All users are in this role by default, whether they have been added directly to the Centrif Directory, or are in an external directory connected through a Centrif Connector.
<input type="checkbox"/> DemoLab	All users are in this role have been added by external directory connected through a Centrif Connector on Demo Lab.
<input type="checkbox"/> EntLab	All users are in this role have been added by external directory connected through a Centrif Connector on Enterprise Lab.
<input type="checkbox"/> System Administrator	The primary administrative role for the Admin Portal. Users in this role can delegate specific administrative rights to other roles who require more limited administrative access.
<input type="checkbox"/> Invited Users	This role is created as part of invite user action. The role is assigned to a proper policy and application for invited users.

Figure 6: Adding Roles.



Centrify Cloud Manager provides Mobile Device Management with FortiGate and FortiAP.

You can centrally configure security and access policies for all wired and wireless users. You can centrally manage devices (info, lock, wipe) and Fortinet App directly to the mobile devices from Centrify.

Fortinet Configuration

For this MDM integration, there is no requirement to configure the FortiGate device.

Fortinet RADIUS Authentication

For RADIUS Authentication, FortiGate can be configured to work with Centrify Cloud as an external RADIUS Server.

Mobile Device Configuration

Install and launch the Centrify application on the mobile device. The user account gets verified against Centrify Cloud Service.

Dashboard and Reporting

The dashboard gives an overview of the login attempts, security events, locations, and devices in the network, as shown in the figure below.

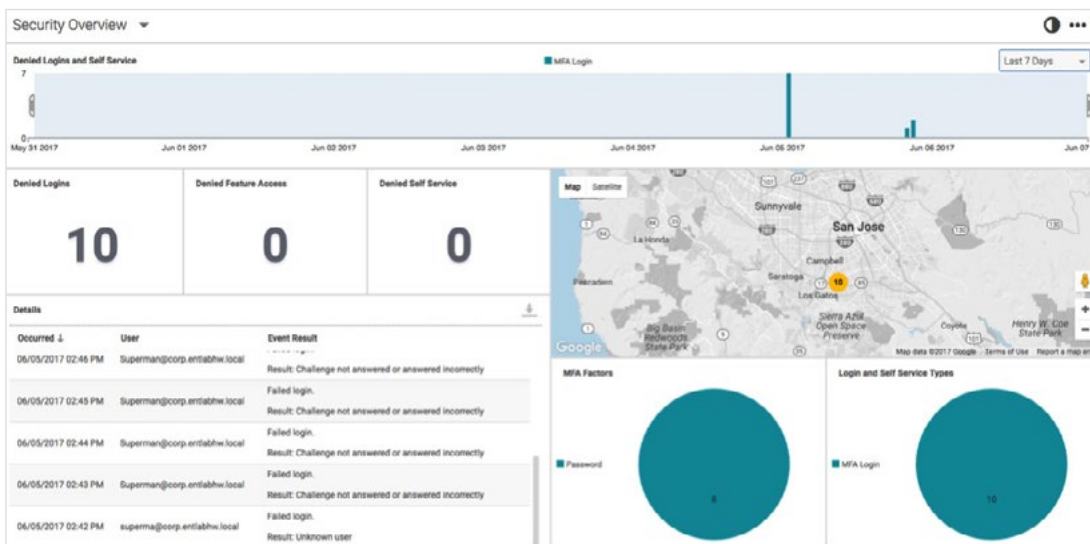


Figure 7: Dashboard.

The Users tab under Core Services lists the status of the authorized users.

Login Name	Display Name	Email	Source	Status	Last Invite	Last Login
<input type="checkbox"/> admin_tm@fortinet.com.76	admin_tm@	tm@fortinet.com	Centrify Directory	Active		06/06/2017 9:33:51 AM
<input type="checkbox"/> adrianaaceva@corp.fortidemo...	Adriana L.A. Ceiva		Active Directory (corp.fortidemo...	Active		02/01/2017 5:08:47 AM
<input type="checkbox"/> anthony soprano@corp.fortidemo...	Anthony Soprano		Active Directory (corp.fortidemo...	Active		01/31/2017 5:00:23 PM
<input type="checkbox"/> artiebucos@corp.fortidemo.com	Artie Bucos		Active Directory (corp.fortidemo...	Active		01/31/2017 4:37:44 PM
<input type="checkbox"/> bane@corp.entlabhw.local	Bane		Active Directory (corp.EntLabH...	Active		06/07/2017 7:01:04 AM
<input type="checkbox"/> carbonblack@corp.entlabhw.local	carbonblack		Active Directory (corp.EntLabH...	Not Invited		
<input type="checkbox"/> carmelasoprano@corp.fortidemo...	Carmela Soprano		Active Directory (corp.fortidemo...	Active		02/22/2017 6:12:27 AM
<input type="checkbox"/> joker@corp.entlabhw.local	Joker		Active Directory (corp.EntLabH...	Active		02/01/2017 2:35:45 PM
<input type="checkbox"/> superman@corp.entlabhw.local	Super Man		Active Directory (corp.EntLabH...	Active		06/07/2017 11:52:18 AM

Figure 8: User.



The Apps tab lists the apps that can be deployed and the status of those apps.

Name	Type	Description	Provisioning	App Gateway	Status
Centrifly	iOS - App Store	The Centrifly mobile app provides you with secure convenient access to all your organization's...			Ready to Deploy
Centrifly Mobile	Android - App Store	Centrifly Mobile is the perfect companion for business travel. You can capture receipts and exp...			Ready to Deploy
FortiClient	iOS - App Store	FortiClient App includes the following features: SSLVPN allows you to create a secure SSL V...			Ready to Deploy
FortiClient	Android - App Store	The new FortiClient v5.4 Endpoint Security App not only allows you to securely connect to For...			Deployed
FortiClient VPN	Android - App Store	This FortiClient VPN App allows you to create a secure Virtual Private Network (VPN) connect...			Ready to Deploy
FortiExplorer Lite	iOS - App Store	FortiExplorer Lite App is a user-friendly configuration tool that helps you to quickly and easily...			Ready to Deploy
FortiLink	Android - App Store	Welcome to the Fortinet Portal. Get the latest Fortinet information, including sales, marketing, ...			Ready to Deploy
Fortinet XTREME 2016	Android - App Store	WHAT IS THE FORTINET XTREME? The 10th edition of the LATAM XTrame Event brings a mo...			Ready to Deploy
FortiRecorder Mobile	Android - App Store	FortiRecorder Mobile Android App is a user-friendly tool that lets you access your FortiRecor...			Ready to Deploy
FortiRecorder Mobile	iOS - App Store	FortiRecorder Mobile iOS App is a user-friendly client that lets you access your FortiRecor...			Ready to Deploy
FortiToken Mobile	iOS - App Store	FortiToken Mobile is an OATH compliant, event-based and time-based One Time Password (O...			Ready to Deploy
FortiToken Mobile	Android - App Store	FortiToken Mobile is an OATH compliant, time-based and event-based One Time Password (O...			Ready to Deploy
FortiWLM App	iOS - App Store	FortiWLM is a network manager application which manages wireless networks in an enterpris...			Ready to Deploy
ISCharlot Endpoint	iOS - App Store	Isa's ISCharlot software endpoint, in combination with Isa's ISCharlot or HawkEye (formerly Is...			Ready to Deploy
User Portal	Web - Portal	The User Portal is your interface to the Centrifly Identity Platform. From the portal, you open w...			Deployed

Figure 7: Dashboard.

The Endpoints tab lists the status of the authorized device, the apps installed, and details of the hardware, as shown below.

Name	Serial	Model Name	OS Version	User	Owner	Carrier	Phone Number	Compliance	Status
XT830C (PN: 0000006532)	ZX1P02J7G	XT830C	4.4.4	AdrianaLaCena@corp.fortidemo...	Personal		0000006532	Compliant	Unreach...
XT830C (PN: 0000001122)	ZX1P02D7PV	XT830C	4.4.4	AnthonySoprano@corp.fortidem...	Personal		0000001122	Compliant	Unreach...
BLU Advance 5.0 (PN: 01234567...)	0123456789...	BLU Advance 5.0	5.1	ArtBuccio@corp.fortidemo.com	Personal				Unenrolld
XT830C (PN: 0000008551)	ZX1P02BMM	XT830C	4.4.4	Bane@corp.entlabw.local	Personal		0000008551	Compliant	Enrolld
XT830C (PN: 0000001122)	ZX1P02D7PV	XT830C	4.4.4	CarmeloSoprano@corp.fortidem...	Personal		0000001122	Compliant	Unreach...
BLU Advance 5.0 (PN: 01234567...)	0123456789...	BLU Advance 5.0	5.1	Joker@corp.entlabw.local	Personal				Unenrolld
Moto 0 Play (SN: ZY2323GVQF2)	ZY2323GVQF2	Moto 0 Play	6.0.1	Superman@corp.entlabw.local	Personal			Compliant	Enrolld

Figure 8: User.

Summary

Access to Centrifly Demo: This demo is part of FortiDemo and EntLab portal and can be accessed using <https://aap0764.my.centrifly.com/>. Log in as admin/admin.

How To Get Help

Fortinet:

This demo is part of the EntLab portal. Contact the Technical Marketing Group to access the setup.

- <https://fuse.fortinet.com/p/do/sd/sid=2302&fid=3542&req=direct>
- tmg@fortinet.com

Centrifly:

- <https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Fortinet-Centrifly.pdf>
- <http://community.centrifly.com/centrifly/attachments/centrifly/techblog/537/1/Centrifly%20for%20Fortinet%20RADIUS%20configuration%20guide.pdf>
- support@centrifly.com



www.fortinet.com

Copyright © 2021 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.