

GUIDE – SEPTEMBER 2018

PRINTED 11 JANUARY 2019

SUMMARY AND ADDITIONAL RESOURCES

VMware Workspace ONE

Table of Contents

[Summary and Additional Resources](#)

- [Conclusion](#)
- [Terminology Used in This Tutorial](#)
- [About the Authors](#)
- [Feedback](#)

Deploying VMware Unified Access Gateway: VMware Workspace ONE Operational Tutorial

Summary and Additional Resources

Conclusion

In these exercises, you have learned how to:

- Deploy the VMware Unified Access Gateway on one NIC using the vSphere Web Client
- Access the VMware Unified Access Gateway administration console
- Configure TLS Certificate for the Unified Access Gateway administrative and Internet interfaces
- Change network settings from Unified Access Gateway administration console

For additional documentation, be sure to check out the VMware Unified Access Gateway Reference page at <https://docs.vmware.com/en/Unified-Access-Gateway/>

Terminology Used in This Tutorial

The following terms are used in this tutorial:

application store	A user interface (UI) framework that provides access to a self-service catalog, public examples of which include the Apple App Store, the Google Play Store, and the Microsoft Store.
auto-enrollment	Auto-enrollment simplifies the enrollment process by automatically enrolling registered devices following the Out-of-Box-Experience.
catalog	A user interface (UI) that displays a personalized set of virtual desktops and applications to users and administrators. These resources are available to be launched upon selection.
cloud	Asset of securely accessed, network-based services and applications. A cloud can also host data storage. Clouds can be private or public, as well as hybrid, which is both private and public.
device enrollment	The process of installing the mobile device management agent on an authorized device. This allows access to VMware products with application stores, such as VMware Identity Manager.
identity provider (IdP)	A mechanism used in a single-sign-on (SSO) framework to automatically give a user access to a resource based on their authentication to a different resource.
mobile device management (MDM) agent	Software installed on an authorized device to monitor, manage, and secure end-user access to enterprise resources.
one-touch login	A mechanism that provides single sign-on (SSO) from an authorized device to enterprise resources.
service provider (SP)	A host that offers resources, tools, and applications to users and devices.
virtual desktop	The user interface of a virtual machine that is made available to an end user.
virtual machine	A software-based computer, running an operating system or application environment, that is located in the data center and backed by the resources of a physical computer.

For more information, see the [VMware Glossary](#).

About the Authors

This tutorial was written by:

- Andreano Lanusse, End-User-Computing Staff Architect, Technical Marketing, VMware.

Feedback

The purpose of this tutorial is to assist you. Your feedback is valuable. To comment on this tutorial, contact VMware End-User-Computing Technical Marketing at euc_tech_content_feedback@vmware.com.



vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
Copyright © 2017 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at <http://www.vmware.com/go/patents>. VMware is a registered trademark or trademark of VMware, Inc. in the United States and/or other jurisdictions. All other marks and names mentioned herein may be trademarks of their respective companies.