DEPLOYMENT GUIDE

Setting Up a Kerberos Relay for the Microsoft Exchange 2013 Server

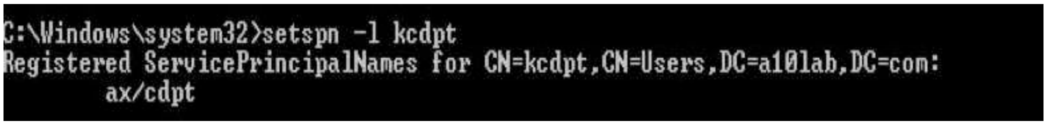
Disclaimer

This document does not create any express or implied warranty about A10 Networks or about its products or services, including but not limited to fitness for a particular use and noninfringement. A10 Networks has made reasonable efforts to verify that the information contained herein is accurate, but A10 Networks assumes no responsibility for its use. All information is provided "as-is." The product specifications and features described in this publication are based on the latest information available; however, specifications are subject to change without notice, and certain features may not be available upon initial product release. Contact A10 Networks for current information regarding its products or services. A10 Networks' products and services are subject to A10 Networks' standard terms and conditions.

To set up a Kerberos relay for the Microsoft Exchange 2013 server:

1. Create an account for A10 Networks® Thunder® Series and set an SPN for this account.

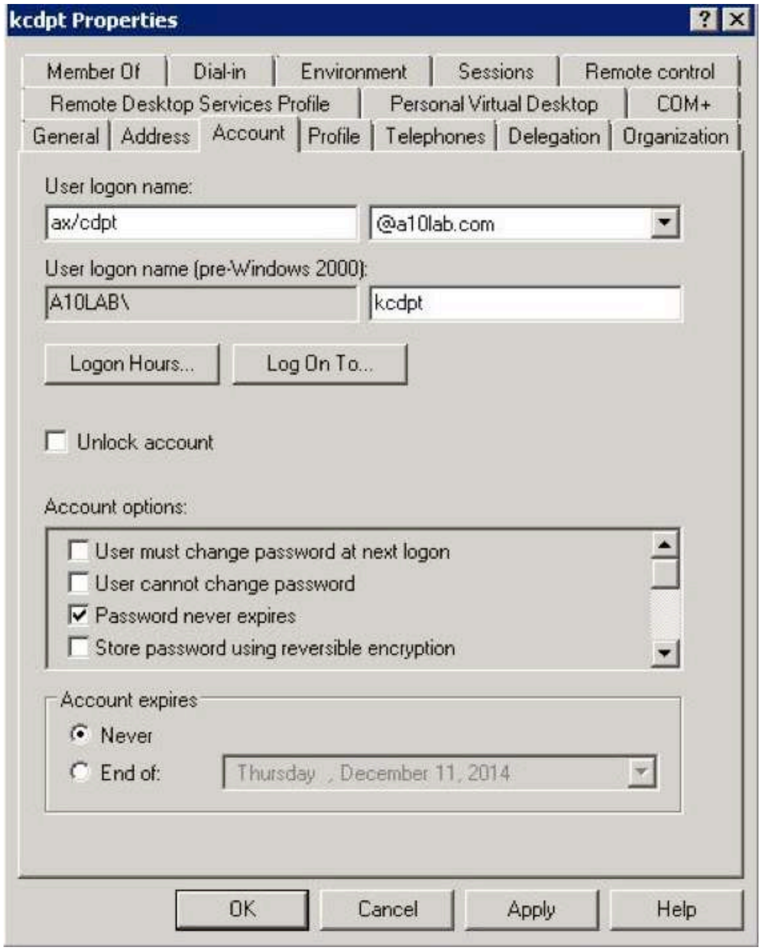
   In the example in Figure 1, the account name is *kcdpt* and service principal name (SPN) is *ax/cdpt*.



```
C:\Windows\system32>setspn -l kcdpt
Registered ServicePrincipalNames for CN=kcdpt,CN=Users,DC=a10lab,DC=com:
        ax/cdpt
```

Figure 1: Account name

2. Ensure that the user logon name of the account is same as the SPN.



User logon name: ax/cdpt @a10lab.com

User logon name (pre-Windows 2000): A10LAB\ kcdpt

□ Unlock account

Account options:

- □ User must change password at next logon
- □ User cannot change password
- ☑ Password never expires
- □ Store password using reversible encryption

Account expires

- ● Never
- ○ End of: Thursday , December 11, 2014

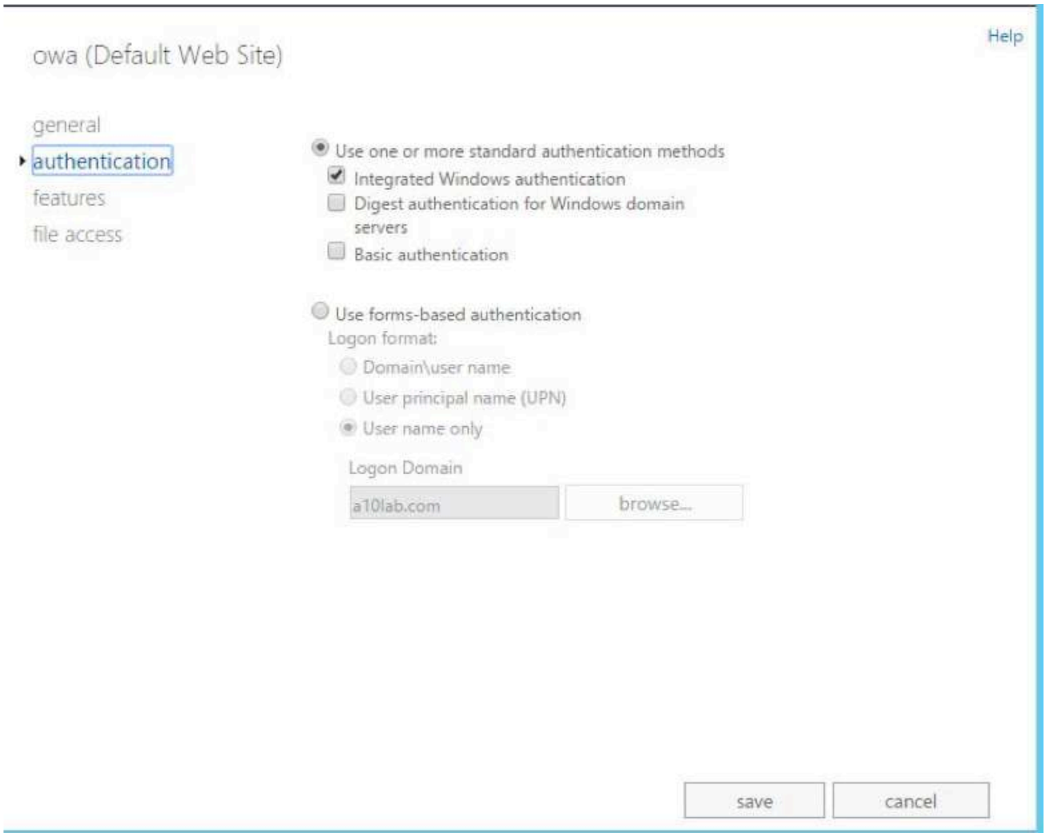
Figure 2: Account details tab

3. On the Thunder Series, configure the SPN of *kcdpt* by entering the following commands:

   In the following example, *ax/cdpt* under Kerberos-account setting in the Kerberos-relay. The password field is the password of the *kcdpt* account, and the Kerberos-realm is the Active Directory (AD) domain name in capital letters:

```
aam authentication relay kerberos krb-relay
  kerberos-realm A10LAB.COM
  kerberos-kdc 192.168.221.50
  kerberos-account ax/cdpt
  password encrypted
u40dcApRH0TD6HSpiq1PHjwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
```

4. On the Exchange server and log in in to the Exchange administrator center.
5. Click **Servers** > **Virtual Directories**.
6. Edit the OWA virtual directory.
7. Go to the Authentication tab and select Use one or more standard authentication methods.
8. Select the Integrated Windows authentication checkbox.



owa (Default Web Site)

● Use one or more standard authentication methods

☑ Integrated Windows authentication

□ Digest authentication for Windows domain servers

□ Basic authentication

○ Use forms-based authentication

Logon format:

○ Domain\user name

○ User principal name (UPN)

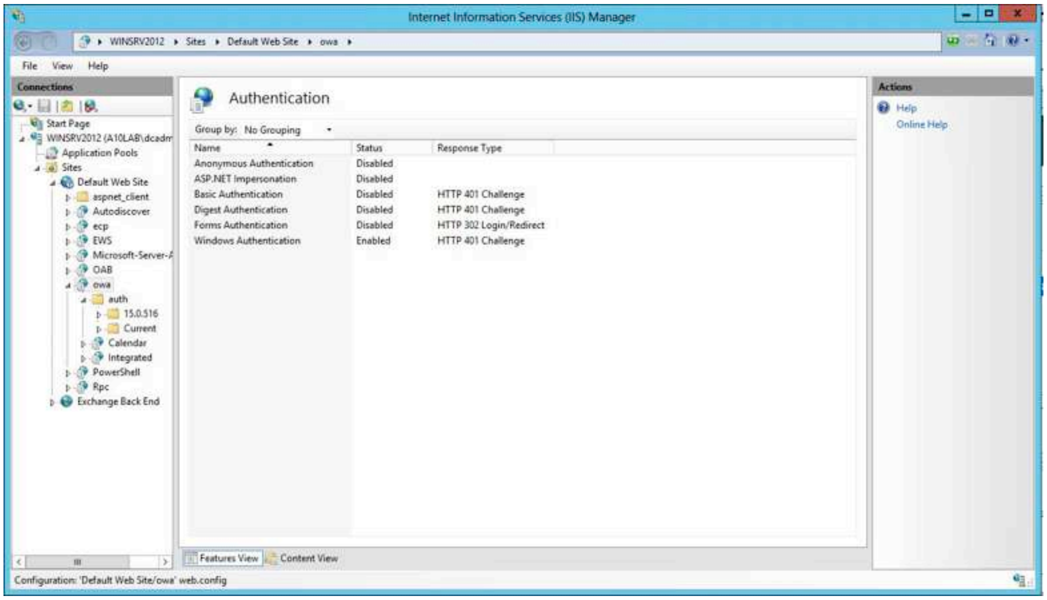
● User name only

Logon Domain: a10lab.com

Figure 3: Editing the OWA virtual directory

The same settings also apply to the ECP virtual directory.

9. On the PowerShell, enter the following commands to restart the IIS server on the Exchange server. The restart of the IIS services is required on all exchange servers after making any authentication settings on the Exchange server.
   - iisreset/noforce
10. In the **Authentication** tab, review the settings on the OWA virtual directory.



Authentication

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Disabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

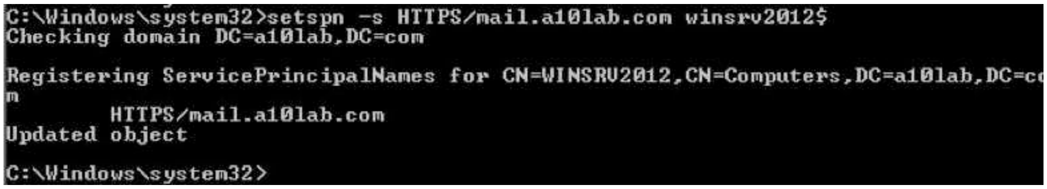
Configuration: 'Default Web Site/owa' web.config

Figure 4: Reviewing the OWA settings

If the settings are not the same, you can manually alter the settings on this page and enter the **iisreset** command again. Make sure that anonymous authentication is also enabled for the ECP virtual-directory.

11. Add an SPN in the format service/*fqdn* for the Exchange server's computer account.

    In the example in Figure 5, the Exchange server's computer account is *winsrv2012*.



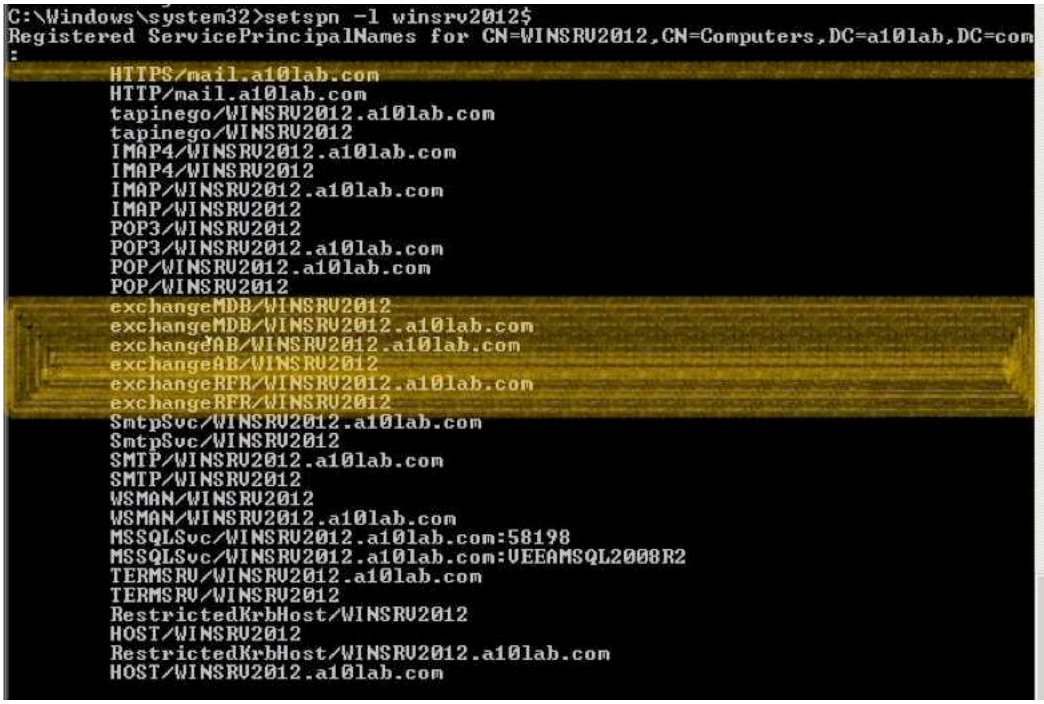
```
C:\Windows\system32>setspn -s HTTPS/mail.a10lab.com winsrv2012$
Checking domain DC=a10lab,DC=com

Registering ServicePrincipalNames for CN=WINSRV2012,CN=Computers,DC=a10lab,DC=c
m
        HTTPS/mail.a10lab.com
Updated object

C:\Windows\system32>
```

Figure 5: Computer account for the Exchange server

The configured SPN goes under the *service-principal-name* section of the SLB server:

```
slb server exchange 192.168.230.84
  port 443 tcp
    service-principal-name HTTPS/mail.a10lab.com
```

You must ensure that the highlighted SPN's exist under this account:

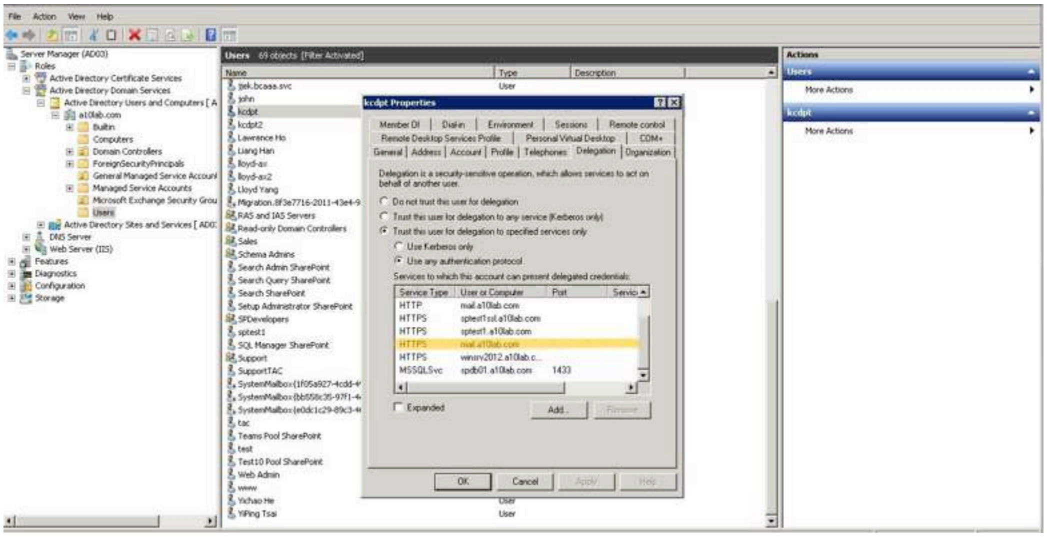


```
C:\Windows\system32>setspn -l winsrv2012$
Registered ServicePrincipalNames for CN=WINSRV2012,CN=Computers,DC=a10lab,DC=com
:
        HTTPS/mail.a10lab.com
        HTTP/mail.a10lab.com
        tapinego/WINSRV2012.a10lab.com
        tapinego/WINSRV2012
        IMAP4/WINSRV2012.a10lab.com
        IMAP4/WINSRV2012
        IMAP/WINSRV2012.a10lab.com
        IMAP/WINSRV2012
        POP3/WINSRV2012
        POP3/WINSRV2012.a10lab.com
        POP/WINSRV2012.a10lab.com
        POP/WINSRV2012
        exchangeMDB/WINSRV2012
        exchangeMDB/WINSRV2012.a10lab.com
        exchangeAB/WINSRV2012.a10lab.com
        exchangeAB/WINSRV2012
        exchangeRFR/WINSRV2012.a10lab.com
        exchangeRFR/WINSRV2012
        SmtpSvc/WINSRV2012.a10lab.com
        SmtpSvc/WINSRV2012
        SMTP/WINSRV2012.a10lab.com
        SMTP/WINSRV2012
        WSMAN/WINSRV2012
        WSMAN/WINSRV2012.a10lab.com
        MSSQLSvc/WINSRV2012.a10lab.com:58198
        MSSQLSvc/WINSRV2012.a10lab.com:VEEAMSQL2008R2
        TERMSRV/WINSRV2012.a10lab.com
        TERMSRV/WINSRV2012
        RestrictedKrbHost/WINSRV2012
        HOST/WINSRV2012
        RestrictedKrbHost/WINSRV2012.a10lab.com
        HOST/WINSRV2012.a10lab.com
```

Figure 5: SPNs in the account

In the example in Figure 5, *winsrv2012.a10lab.com* is the internal URL for the exchange server. If SPNs are not present, see http://blogs.technet.com/b/kpapadak/archive/2011/03/13/setting-up-kerberos-with-a-client-access-server-array.aspx for more information about creating a service account and associating the account to an Exchange server.

12. Delegate control to the Thunder Series account, *kcdpt*, to handle the tickets for the Exchange server by adding the Exchange server's SPN to the Thunder Series account.



Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this user for delegation
○ Trust this user for delegation to any service (Kerberos only)
● Trust this user for delegation to specified services only
○ Use Kerberos only
● Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Servic
HTTP	mail.a10lab.com		
HTTPS	sptest1ssl.a10lab.com		
HTTPS	sptest1.a10lab.com		
HTTPS	mail.a10lab.com		
HTTPS	winsrv2012.a10lab.c...		
MSSQLSvc	spdb01.a10lab.com	1433	

□ Expanded

Figure 6: Delegating control to the Thunder Series account

The sample configuration also includes setting for Microsoft SharePoint:

```
TH4430#sh run
!Current configuration: 900 bytes
!Configuration last updated at 21:40:42 PST Mon Nov 10 2014
!Configuration last saved at 21:40:42 PST Mon Nov 10 2014
!64-bit Advanced Core OS (ACOS) version 4.0.0, build 489 (Nov-07-2014,09:03)
!
partition p1 id 1
!
!
timezone America/Los_Angeles
!
!
interface management
  ip address 192.168.230.45 255.255.255.0
  ip default-gateway 192.168.230.254
!
!
interface ethernet 1
!
interface ethernet 2
!
interface ethernet 3
  enable
  ip address 192.168.231.21 255.255.255.0
!
interface ethernet 4
!
interface ethernet 5
!
interface ethernet 6
!
interface ethernet 7
!
interface ethernet 8
  enable
  ip address 10.50.50.1 255.255.255.0
!
interface ethernet 9
!
interface ethernet 10
!
interface ethernet 11
!
interface ethernet 12
!
!
!
ip route 0.0.0.0 /0 192.168.231.254
!
!
aam authentication server ldap dummy
!
!
aam authentication server ocsp ocsp_serv
```

```
  url http://192.168.230.101:80/ocsp
!
!
!
slb template server-ssl s1
!
!
slb server exchange 192.168.230.84
  port 80 tcp
    service-principal-name HTTP/mail.a10lab.com
  port 443 tcp
    service-principal-name HTTPS/mail.a10lab.com
!
slb server sptest1 192.168.221.100
  port 80 tcp
    service-principal-name HTTP/sptest1.a10lab.com
  port 443 tcp
    service-principal-name HTTPS/sptest1ssl.a10lab.com
  port 8888 tcp
    service-principal-name HTTP/sptest1.a10lab.com
!
!
aam authentication relay kerberos krb-relay
  kerberos-realm A10LAB.COM
  kerberos-kdc 192.168.221.50
  kerberos-account ax/cdpt
  password encrypted
u40dcApRH0TD6HSpiq1PHjwQjLjV2wDnPBCMuNXbAOc8EIy41dsA5zwQjLjV2wDn
!
!
aam authentication template kltest
  relay krb-relay
  server dummy
!
!
aam aaa-policy my-aaa-policy
  aaa-rule 1
    action allow
    authentication-template kltest
!
!
slb service-group exch-443 tcp
  member exchange 443
!
slb service-group exch-80 tcp
  member exchange 80
!
slb service-group mywsu-sg-443 tcp
  member sptest1 443
!
slb service-group mywsu-sg-80 tcp
  member sptest1 80
!
slb service-group mywsu-sg-8888 tcp
  member sptest1 8888
!
```

```
!
slb template client-ssl cssl
  auth-username subject-alt-name-othername
  ca-cert AD03-CA
  cert 230.45-cert
  client-certificate Require
  key 230.45-cert
!
slb template client-ssl exch-ssl
  cert 230.45-cert
  key 230.45-cert
!
!
slb virtual-server exchange-vs 192.168.231.22
  port 80 http
    source-nat auto
    service-group exch-80
  port 443 https
    source-nat auto
    service-group exch-443
    template server-ssl s1
    template client-ssl cssl
    aaa-policy my-aaa-policy
!
slb virtual-server sharepoint-vs 192.168.231.234
  port 80 https
    source-nat auto
    service-group mywsu-sg-80
    template client-ssl cssl
    aaa-policy my-aaa-policy
  port 443 https
    source-nat auto
    service-group mywsu-sg-443
    template server-ssl s1
    template client-ssl cssl
    aaa-policy my-aaa-policy
  port 8888 https
    source-nat auto
    service-group mywsu-sg-8888
    template client-ssl cssl
    aaa-policy my-aaa-policy
!
!
multi-config enable
!
!
terminal idle-timeout 0
!
!
end
!Current config commit point for partition 0 is 0 & config mode is classical-
mode

Tickets obtained:
```

```
TH4430#sh aam authentication klist
-----------------------
Ticket cache: MEMORY:krb-relay
Default principal: ax/cdpt@A10LAB.COM

Service principal: HTTPS/mail.a10lab.com@A10LAB.COM
Client principal: dcadmin@A10LAB.COM
timespan: 11:30 11,Nov,2014 - 21:30 11,Nov,2014
renew untill: 11:30 18,Nov,2014
flags: FRA

Service principal: ax/cdpt@A10LAB.COM
Client principal: dcadmin@A10LAB.COM
timespan: 11:30 11,Nov,2014 - 21:30 11,Nov,2014
renew untill: 11:30 18,Nov,2014
flags: FRA

Service principal: krbtgt/A10LAB.COM@A10LAB.COM
Client principal: ax/cdpt@A10LAB.COM
timespan: 11:31 11,Nov,2014 - 21:30 11,Nov,2014
renew untill: 11:31 18,Nov,2014
flags: FRIA

TH4430#
```

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-DG-16145-EN-02
June 2015

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com

Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
Hong Kong
HongKong@a10networks.com
South Asia
SouthAsia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To learn more about the A10 Thunder Application Service Gateways and how it can enhance your business, contact A10 Networks at: **www.a10networks.com/contact** or call to talk to an A10 sales representative.