# Verwalten der SAML-Authentifizierungseinstellungen

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/config/concept_manage_saml_authentication_settings_um.html on November 13, 2026. Always check docs.netapp.com for the latest.

# Inhalt


Verwalten der SAML-Authentifizierungseinstellungen . . . 1
- SAML Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 1
- Verwendung eines Identitätsanbieters in Active IQ Unified Manager . . . 1
  - Unterstützte Verschlüsselungsstandards . . . 1
  - Validierte Identitätsanbieter . . . 1
  - ADFS Konfigurationsanforderungen . . . 1
  - Weitere Konfigurationsanforderungen . . . 2
- SAML Authentifizierung in Active IQ Unified Manager ist aktiviert . . . 2
- Änderung des SAML Authentifizierungs-Identitätsanbieters in Active IQ Unified Manager . . . 4
- Aktualisierung der SAML-Authentifizierungseinstellungen nach einer Änderung des Active IQ Unified Manager Sicherheitszertifikats . . . 4
- SAML Authentifizierung in Active IQ Unified Manager deaktivieren . . . 6
- Die SAML Authentifizierung wird über die Active IQ Unified Manager Wartungskonsole deaktiviert. . . . 6
- Die SAML Authentifizierungsseite in Active IQ Unified Manager kann verwendet werden . . . 7

# Verwalten der SAML-Authentifizierungseinstellungen

## SAML Authentifizierung in Active IQ Unified Manager ist aktiviert

Nachdem Sie die Einstellungen für die Remote-Authentifizierung konfiguriert haben, können Sie die Authentifizierung mit Security Assertion Markup Language (SAML) aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Web-Benutzeroberfläche von Unified Manager zugreifen können.

Nach der Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche von Unified Manager. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Managementplattform für die Wartung zugreifen.

## Verwendung eines Identitätsanbieters in Active IQ Unified Manager

Wenn Unified Manager so konfiguriert wird, dass ein Identitätsanbieter (IdP) die SAML-Authentifizierung für alle Remote-Benutzer durchführt, müssen einige erforderliche Konfigurationseinstellungen beachtet werden, damit die Verbindung zu Unified Manager erfolgreich hergestellt werden kann.

Sie müssen die Unified Manager URI und die Metadaten in den IdP-Server eingeben. Diese Informationen können Sie auf der Unified Manager SAML-Authentifizierungsseite kopieren. Unified Manager gilt im Standard Security Assertion Markup Language (SAML) als Serviceprovider (SP).

### Unterstützte Verschlüsselungsstandards

- Advanced Encryption Standard (AES): AES-128 und AES-256
- Sicherer Hash-Algorithmus (SHA): SHA-1 und SHA-256

### Validierte Identitätsanbieter

- Shibboleth
- Active Directory Federation Services (ADFS)

### ADFS Konfigurationsanforderungen

- Sie müssen drei Anspruchsregeln in der folgenden Reihenfolge definieren, die erforderlich sind, damit Unified Manager ADFS SAML-Antworten für diesen Vertrauensstellungseintrag der vertrauenden Seite analysieren kann.

| Claim-Regel | Wert |
| --- | --- |
| SAM-Kontoname | Name-ID |
| SAM-Kontoname | urn:oid:0.9.2342.19200300.100.1.1 |
| Tokengruppen — Unqualifizierter Name | urn:oid:1.3.6.1.4.1.5923.1.5.1.1 |

- Sie müssen das Authentifizierungsverfahren auf “Forms Authentication” festlegen, da Benutzer sonst beim Abmelden von Unified Manager eine Fehlermeldung erhalten können. Die folgenden Schritte sind erforderlich:
  a. Die ADFS Management Console wird geöffnet.
  b. In der linken Baumansicht den Ordner „Authentifizierungsrichtlinien“ auswählen.
  c. Rechts unter „Aktionen“ befindet sich die Option „Globale primäre Authentifizierungsrichtlinie bearbeiten“.
  d. Als Authentifizierungsverfahren für das Intranet wird statt der Standardeinstellung “Windows Authentication” die Option “Forms Authentication” verwendet.
- In einigen Fällen wird die Anmeldung über den IdP abgelehnt, wenn das Sicherheitszertifikat des Unified Manager CA-signiert ist. Es gibt zwei Lösungsansätze für dieses Problem:
  - Im Link finden Sie Anweisungen zum Deaktivieren der Widerrufsprüfung auf dem ADFS-Server für verkettete CA-Zertifikate der zugeordneten Relying Party:

    "Widerrufsprüfung pro Relying Party Trust deaktivieren"

  - Der CA-Server muss sich innerhalb des ADFS-Servers befinden, um die Zertifikatsanforderung des Unified Manager Servers zu signieren.

### Weitere Konfigurationsanforderungen

- Die Taktabweichung von Unified Manager ist auf 5 Minuten eingestellt, daher darf die Zeitdifferenz zwischen dem IdP-Server und dem Unified Manager-Server nicht mehr als 5 Minuten betragen, da die Authentifizierung sonst fehlschlägt.

# SAML Authentifizierung in Active IQ Unified Manager ist aktiviert

Sie können die Security Assertion Markup Language (SAML) Authentifizierung aktivieren, sodass Remote-Benutzer von einem sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie auf die Unified Manager Weboberfläche zugreifen können.

**Bevor Sie beginnen**

- Sie müssen die Remote-Authentifizierung konfiguriert und überprüft haben, dass sie erfolgreich ist.
- Sie müssen mindestens einen Remote User oder eine Remote Group mit der Rolle Application Administrator erstellt haben.
- Der Identitätsanbieter (IdP) muss von Unified Manager unterstützt werden und konfiguriert sein.
- Sie benötigen die IdP-URL und die Metadaten.
- Sie benötigen Zugriff auf den IdP-Server.

Nachdem Sie die SAML-Authentifizierung in Unified Manager aktiviert haben, können Benutzer erst dann auf

die grafische Benutzeroberfläche zugreifen, wenn der IdP mit den Hostinformationen des Unified Manager Servers konfiguriert wurde. Daher ist es erforderlich, beide Teile der Verbindung abzuschließen, bevor der Konfigurationsprozess gestartet wird. Der IdP kann vor oder nach der Konfiguration von Unified Manager eingerichtet werden.

Nach der Aktivierung der SAML-Authentifizierung haben nur Remote-Benutzer Zugriff auf die grafische Benutzeroberfläche des Unified Manager. Lokale Benutzer und Wartungsbenutzer können nicht auf die Benutzeroberfläche zugreifen. Diese Konfiguration hat keine Auswirkungen auf Benutzer, die auf die Managementplattform, die Unified Manager-Befehle oder die ZAPIs zugreifen.

Unified Manager wird automatisch neu gestartet, nachdem Sie die SAML-Konfiguration auf dieser Seite abgeschlossen haben.

**Schritte**

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Das Kontrollkästchen **SAML-Authentifizierung aktivieren** ist auszuwählen.

   Die für die Konfiguration der IdP-Verbindung erforderlichen Felder werden angezeigt.

3. Einzugeben sind die IdP URI und die IdP Metadaten, die für die Verbindung des Unified Manager Servers mit dem IdP Server erforderlich sind.

   Wenn der IdP-Server direkt vom Unified Manager Server aus erreichbar ist, können Sie nach Eingabe der IdP URI auf die Schaltfläche **Fetch IdP Metadata** klicken, um das Feld „IdP Metadata“ automatisch zu füllen.

4. Die Host-Metadaten-URI von Unified Manager kann kopiert oder die Host-Metadaten können in einer XML-Textdatei gespeichert werden.

   Sie können den IdP-Server jetzt mit diesen Informationen konfigurieren.

5. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

6. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, müssen sie ihre Anmeldeinformationen auf der IdP-Anmeldeseite anstatt auf der Unified Manager-Anmeldeseite eingeben.

Falls dies noch nicht geschehen ist, sind für den Abschluss der Konfiguration der Zugriff auf Ihren IdP sowie die Eingabe der URI und der Metadaten des Unified Manager Servers erforderlich.

Wenn Sie ADFS als Identitätsanbieter verwenden, beachtet die Unified Manager GUI die ADFS-Zeitüberschreitung nicht und funktioniert weiter, bis die Unified Manager Sitzungs-Zeitüberschreitung erreicht ist. Die Zeitüberschreitung der GUI-Sitzung kann durch Klicken auf **General** > **Feature Settings** > **Inactivity Timeout** geändert werden.

# Änderung des SAML Authentifizierungs-Identitätsanbieters in Active IQ Unified Manager

Sie können den Identitätsanbieter (IdP) ändern, den Unified Manager zur Authentifizierung von Remote-Benutzern verwendet.

**Bevor Sie beginnen**

- Sie benötigen die IdP-URL und die Metadaten.
- Sie benötigen Zugriff auf den Identitätsanbieter (IdP).

Der neue IdP lässt sich vor oder nach der Konfiguration von Unified Manager konfigurieren.

**Schritte**

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Einzugeben sind die neue IdP URI sowie die IdP-Metadaten, die für die Verbindung des Unified Manager server mit dem IdP erforderlich sind.

   Wenn der IdP direkt vom Unified Manager Server aus erreichbar ist, können Sie nach Eingabe der IdP URL auf die Schaltfläche **Fetch IdP Metadata** klicken, um das Feld „IdP Metadata“ automatisch auszufüllen.

3. Sie können den Unified Manager Metadaten-URI kopieren oder die Metadaten in einer XML-Textdatei speichern.
4. Im nächsten Schritt erfolgt die Auswahl von **Konfiguration speichern**.

   Ein Meldungsfeld wird angezeigt, um zu bestätigen, dass Sie die Konfiguration ändern möchten.

5. Klicken Sie auf **OK**.

Zum Abschließen der Konfiguration auf den neuen IdP zugreifen und die Unified Manager Server-URI sowie die Metadaten eingeben.

Wenn autorisierte Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, müssen sie ihre Anmeldeinformationen auf der neuen IdP-Anmeldeseite anstatt auf der alten IdP-Anmeldeseite eingeben.

# Aktualisierung der SAML-Authentifizierungseinstellungen nach einer Änderung des Active IQ Unified Manager Sicherheitszertifikats

Jede Änderung des auf dem Unified Manager Server installierten HTTPS-Sicherheitszertifikats erfordert eine Aktualisierung der SAML Authentifizierungskonfigurationseinstellungen. Das Zertifikat wird aktualisiert, wenn Sie das Hostsystem umbenennen, ihm eine neue IP-Adresse zuweisen oder das Sicherheitszertifikat für das System manuell ändern.

Nach der Änderung des Sicherheitszertifikats und dem Neustart des Unified Manager Servers funktioniert die SAML Authentifizierung nicht mehr, und Benutzer können nicht auf die grafische Benutzeroberfläche des Unified Manager zugreifen. Um den Zugriff auf die Benutzeroberfläche wiederherzustellen, müssen Sie die

SAML Authentifizierungseinstellungen sowohl auf dem IdP Server als auch auf dem Unified Manager Server aktualisieren.

**Schritte**

1. Bei der Wartungs-Managementplattform erfolgt die Anmeldung.
2. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **SAML-Authentifizierung deaktivieren**.

   Es erscheint eine Meldung zur Bestätigung, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Die Unified Manager Benutzeroberfläche kann über den aktualisierten FQDN oder die IP-Adresse aufgerufen werden. Dabei wird das aktualisierte Serverzertifikat im Browser akzeptiert, und die Anmeldung erfolgt mit den Anmeldedaten des Wartungsbenutzers.
4. Die Konfiguration der IdP-Verbindung erfolgt auf der Seite **Setup/Authentifizierung** über die Registerkarte **SAML-Authentifizierung**.
5. Die Host-Metadaten-URI von Unified Manager kann kopiert oder die Host-Metadaten können in einer XML-Textdatei gespeichert werden.
6. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

7. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.
8. Zum Abschluss der Konfiguration erfolgt auf dem IdP-Server die Eingabe der URI des Unified Manager-Servers und der Metadaten.

| Identitätsanbieter | Konfigurationsschritte |
|---|---|
| ADFS | a. In der ADFS-Management-GUI erfolgt das Löschen des vorhandenen Eintrags für die Vertrauensstellung der vertrauenden Seite.<br>b. Das Hinzufügen eines neuen Eintrags für die Vertrauensstellung der vertrauenden Seite erfolgt mithilfe des `saml_sp_metadata.xml` aktualisierten Unified Manager Servers.<br>c. Definition der drei Anspruchsregeln, die Unified Manager benötigt, um ADFS SAML-Antworten für diesen Eintrag der Vertrauensstellung der vertrauenden Seite zu analysieren.<br>d. Ein Neustart des ADFS Windows Service ist erforderlich. |
| Shibboleth | a. Der neue FQDN des Unified Manager Servers ist in den `attribute-filter.xml` und `relying-party.xml` Dateien zu aktualisieren.<br>b. Nach dem Neustart des Apache Tomcat Webservers ist zu warten, bis Port 8005 online ist. |

9. Nach der Anmeldung bei Unified Manager sollte überprüft werden, ob die SAML-Authentifizierung über

Ihren IdP wie erwartet funktioniert.

# SAML Authentifizierung in Active IQ Unified Manager deaktivieren

Sie können die SAML Authentifizierung deaktivieren, wenn die Authentifizierung von Remote-Benutzern über einen sicheren Identitätsanbieter (IdP) beendet werden soll, bevor sie sich bei der Unified Manager Weboberfläche anmelden können. Wenn die SAML Authentifizierung deaktiviert ist, übernehmen die konfigurierten Verzeichnisdienstanbieter, wie z. B. Active Directory oder LDAP, die Anmeldeauthentifizierung.

Nach der Deaktivierung der SAML-Authentifizierung können neben den konfigurierten Remote-Benutzern auch lokale Benutzer und Wartungsbenutzer auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML-Authentifizierung auch über die Unified Manager Managementplattform deaktivieren, wenn Sie keinen Zugriff auf die grafische Benutzeroberfläche haben.

Unified Manager wird nach der Deaktivierung der SAML-Authentifizierung automatisch neu gestartet.

**Schritte**

1. Im linken Navigationsbereich wählen Sie **General** > **SAML Authentication** aus.
2. Das Häkchen im Kontrollkästchen **SAML-Authentifizierung aktivieren** wird entfernt.
3. Auf **Speichern** klicken.

   Ein Meldungsfeld erscheint zur Bestätigung, dass Sie die Konfiguration abschließen und Unified Manager neu starten möchten.

4. Nach einem Klick auf **Confirm and Logout** wird Unified Manager neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der Unified Manager Anmeldeseite statt auf der IdP Anmeldeseite ein.

Sie greifen auf Ihren IdP zu und löschen die Unified Manager Server URI und die Metadaten.

# Die SAML Authentifizierung wird über die Active IQ Unified Manager Wartungskonsole deaktiviert.

Möglicherweise ist es erforderlich, die SAML Authentifizierung über die Managementplattform zu deaktivieren, wenn kein Zugriff auf die Unified Manager GUI besteht. Dies kann bei Fehlkonfigurationen oder wenn der Identitätsanbieter (IdP) nicht erreichbar ist, der Fall sein.

**Bevor Sie beginnen**

Sie müssen als Wartungsbenutzer Zugriff auf die Managementplattform haben.

Wenn die SAML-Authentifizierung deaktiviert ist, übernehmen die konfigurierten Verzeichnisdienstanbieter wie Active Directory oder LDAP die Anmeldeauthentifizierung. Lokale Benutzer und Wartungsbenutzer können dann zusätzlich zu den konfigurierten Remote-Benutzern auf die grafische Benutzeroberfläche zugreifen.

Sie können die SAML Authentifizierung auch auf der Seite „Setup/Authentication“ in der UI deaktivieren.

Unified Manager wird nach der Deaktivierung der SAML-Authentifizierung automatisch neu gestartet.

**Schritte**

1. Bei der Wartungs-Managementplattform erfolgt die Anmeldung.
2. Im **Hauptmenü** erfolgt die Eingabe der Nummer für die Option **SAML-Authentifizierung deaktivieren**.

   Es erscheint eine Meldung zur Bestätigung, dass Sie die SAML-Authentifizierung deaktivieren und Unified Manager neu starten möchten.

3. Nach Eingabe von **y** und Drücken der Eingabetaste wird Unified Manager neu gestartet.

Wenn Remote-Benutzer das nächste Mal versuchen, auf die grafische Benutzeroberfläche des Unified Manager zuzugreifen, geben sie ihre Anmeldeinformationen auf der Unified Manager Anmeldeseite statt auf der IdP Anmeldeseite ein.

Falls erforderlich, können Sie auf Ihren IdP zugreifen und die Unified Manager Server-URL sowie die Metadaten löschen.

# Die SAML Authentifizierungsseite in Active IQ Unified Manager kann verwendet werden

Auf der Seite „SAML-Authentifizierung“ können Sie Unified Manager so konfigurieren, dass Remote-Benutzer mithilfe von SAML über einen sicheren Identitätsanbieter (IdP) authentifiziert werden, bevor sie sich bei der Unified Manager Weboberfläche anmelden können.

- Sie müssen über die Rolle „Application Administrator“ verfügen, um die SAML-Konfiguration zu erstellen oder zu ändern.
- Sie müssen die Remote-Authentifizierung konfiguriert haben.
- Mindestens ein Remote-Benutzer oder eine Remote-Gruppe muss konfiguriert sein.

Nachdem die Remote-Authentifizierung und die Remote-Benutzer konfiguriert wurden, können Sie durch Aktivieren des Kontrollkästchens „SAML-Authentifizierung aktivieren“ die Authentifizierung mithilfe eines sicheren Identitätsanbieters aktivieren.

- **IdP-URI**

  Die URI für den Zugriff auf den IdP vom Unified Manager Server. Beispiel-URIs sind unten aufgeführt.

  ADFS Beispiel-URI:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

Shibboleth Beispiel-URI:

`https://centos7.ntap2016.local/idp/shibboleth`

- **IdP-Metadaten**

  Die IdP-Metadaten im XML-Format.

  Wenn die IdP-URL vom Unified Manager Server aus erreichbar ist, können Sie auf die Schaltfläche **IdP-Metadaten abrufen** klicken, um dieses Feld auszufüllen.

- **Hostsystem (FQDN)**

  Der FQDN des Unified Manager Hostsystems, wie er während der Installation definiert wurde. Sie können diesen Wert bei Bedarf ändern.

- **Host-URI**

  Die URI für den Zugriff auf das Unified Manager Hostsystem vom IdP aus.

- **Host-Metadaten**

  Die Metadaten des Hostsystems im XML-Format.

**Copyright-Informationen**

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

**Markeninformationen**

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.