



# **Zertifikate und Authentifizierung**

## **SANtricity 11.6**

NetApp  
February 12, 2024

# Inhalt

- Zertifikate und Authentifizierung ..... 1
  - Zertifikatmanagement ..... 1
  - Zugriffsmanagement ..... 10

# Zertifikate und Authentifizierung

## Zertifikatmanagement

### Konzepte

#### Funktionsweise von Zertifikaten

Zertifikate sind digitale Dateien, die Online-Einheiten wie Websites und Server für eine sichere Kommunikation im Internet identifizieren.

#### Signierte Zertifikate

Zertifikate stellen sicher, dass die Webkommunikation in verschlüsselter Form, privat und unverändert, nur zwischen dem angegebenen Server und dem angegebenen Client übertragen wird. Mit Unified Manager können Sie Zertifikate für den Browser auf einem Host-Managementsystem und die Controller in den ermittelten Speicher-Arrays verwalten.

Ein Zertifikat kann von einer vertrauenswürdigen Behörde signiert werden, oder es kann selbst signiert werden. „Unterzeichnen“ bedeutet einfach, dass jemand die Identität des Eigentümers validiert und festgestellt hat, dass seine Geräte vertrauenswürdig sind. Die Storage Arrays werden mit einem automatisch generierten, selbstsignierten Zertifikat auf jedem Controller ausgeliefert. Sie können weiterhin die selbst signierten Zertifikate verwenden oder CA-signierte Zertifikate für eine sicherere Verbindung zwischen den Controllern und den Host-Systemen erhalten.



Auch wenn CA-signierte Zertifikate einen besseren Schutz bieten (zum Beispiel die Verhinderung von man-in-the-Middle-Angriffen), verlangen sie auch Gebühren, die teuer sein können, wenn Sie ein großes Netzwerk haben. Im Gegensatz dazu sind selbstsignierte Zertifikate weniger sicher, aber sie sind kostenlos. Daher werden selbst signierte Zertifikate am häufigsten für interne Testumgebungen eingesetzt, nicht in Produktionsumgebungen.

Ein signiertes Zertifikat wird von einer Zertifizierungsstelle (CA) validiert, einer vertrauenswürdigen Drittorganisation. Signierte Zertifikate enthalten Angaben über den Eigentümer der Einheit (in der Regel Server oder Website), Datum der Zertifikatausgabe und -Ablauf, gültige Domains für das Unternehmen und eine digitale Signatur bestehend aus Buchstaben und Zahlen.

Wenn Sie einen Browser öffnen und eine Webadresse eingeben, führt Ihr System eine Zertifikatprüfung im Hintergrund durch, um zu bestimmen, ob Sie eine Verbindung zu einer Website herstellen, die ein gültiges, von einer Zertifizierungsstelle signiertes Zertifikat enthält. In der Regel enthält eine mit einem signierten Zertifikat gesicherte Website ein Vorhängeschloss-Symbol und eine https-Bezeichnung in der Adresse. Wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die kein CA-signiertes Zertifikat enthält, zeigt Ihr Browser eine Warnung an, dass die Website nicht sicher ist.

Die CA führt Schritte durch, um Ihre Identität während des Anwendungsprozesses zu überprüfen. Sie senden möglicherweise eine E-Mail an Ihr registriertes Unternehmen, überprüfen Ihre Geschäftsadresse und führen eine HTTP- oder DNS-Verifizierung durch. Wenn der Anwendungsprozess abgeschlossen ist, sendet die Zertifizierungsstelle digitale Dateien zum Laden auf einem Host-Managementsystem. In der Regel umfassen diese Dateien eine Kette des Vertrauens, wie folgt:

- **Root** — an der Spitze der Hierarchie befindet sich das Stammzertifikat, welches einen privaten Schlüssel enthält, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie

nur ein Stammzertifikat.

- **Intermediate** — Abzweigung von der Wurzel sind die Zwischenzertifikate. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
- **Server** — unten in der Kette befindet sich das Server-Zertifikat, welches Ihre spezifische Entität, wie z.B. eine Website oder ein anderes Gerät, identifiziert. Jeder Controller in einem Storage Array benötigt ein separates Serverzertifikat.

### Selbstsignierte Zertifikate

Jeder Controller im Speicher-Array verfügt über ein vorinstalliertes, selbstsigniertes Zertifikat. Ein selbst signiertes Zertifikat ähnelt einem CA-signierten Zertifikat, außer dass es vom Eigentümer des Unternehmens anstelle eines Dritten validiert wird. Wie ein Zertifikat mit einer Zertifizierungsstelle enthält auch ein selbstsigniertes Zertifikat einen eigenen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt und über eine HTTPS-Verbindung zwischen einem Server und einem Client gesendet werden.

Selbstsignierte Zertifikate werden von Browsern nicht „Trusted“. Jedes Mal, wenn Sie versuchen, eine Verbindung zu einer Website herzustellen, die nur ein selbstsigniertes Zertifikat enthält, wird im Browser eine Warnmeldung angezeigt. Sie müssen in der Warnmeldung auf einen Link klicken, der Ihnen die Nutzung der Website ermöglicht. Dadurch akzeptieren Sie im Wesentlichen das selbstsignierte Zertifikat.

### Zertifikate für Unified Manager

Die Unified Manager-Schnittstelle wird mit dem Web Services Proxy auf einem Host-System installiert. Wenn Sie einen Browser öffnen und eine Verbindung zu Unified Manager herstellen möchten, versucht der Browser, durch die Suche nach einem digitalen Zertifikat zu überprüfen, ob der Host eine vertrauenswürdige Quelle ist. Wenn der Browser kein von einer Zertifizierungsstelle signiertes Zertifikat für den Server findet, wird eine Warnmeldung angezeigt. Von dort aus können Sie auf der Website fortfahren, um das selbstsignierte Zertifikat für diese Sitzung zu akzeptieren. Oder Sie können signierte digitale Zertifikate von einer Zertifizierungsstelle erhalten, damit die Warnmeldung nicht mehr angezeigt wird.

### Zertifikate für Controller

Während einer Unified Manager-Sitzung werden möglicherweise zusätzliche Sicherheitsmeldungen angezeigt, wenn Sie versuchen, auf einen Controller zuzugreifen, der kein von einer Zertifizierungsstelle signiertes Zertifikat hat. In diesem Fall können Sie dem selbst signierten Zertifikat dauerhaft vertrauen oder die CA-signierten Zertifikate für die Controller importieren, damit der Web Services Proxy-Server eingehende Clientanforderungen von diesen Controllern authentifizieren kann.

### Terminologie des Zertifikats

Die folgenden Begriffe gelten für das Zertifikatmanagement.

Laufzeit	Beschreibung
CA	Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.

<b>Laufzeit</b>	<b>Beschreibung</b>
CSR	Eine Zertifikatsignierungsanforderung (CSR) ist eine Nachricht, die von einem Antragsteller an eine Zertifizierungsstelle (CA) gesendet wird. Der CSR überprüft die Informationen, die die Zertifizierungsstelle zum ausstellen eines Zertifikats benötigt.
Zertifikat	Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).
Zertifikatskette	Eine Dateihierarchie, die den Zertifikaten eine Sicherheitsschicht hinzufügt. In der Regel umfasst die Kette ein Stammzertifikat oben in der Hierarchie, ein oder mehrere Zwischenzertifikate und die Serverzertifikate, die die Entitäten identifizieren.
Zwischenzertifikat	Ein oder mehrere Zwischenzertifikate verzweigen von der Root in der Zertifikatskette. Die CA gibt ein oder mehrere Zwischenzertifikate aus, die als Zwischenzertifikate zwischen geschützten Root- und Serverzertifikaten fungieren sollen.
Schlüsselspeicher	Ein Schlüsselspeicher ist ein Repository auf Ihrem Host-Managementsystem, das private Schlüssel enthält, zusammen mit ihren entsprechenden öffentlichen Schlüsseln und Zertifikaten. Diese Schlüssel und Zertifikate identifizieren Ihre eigenen Einheiten, z. B. die Controller.
Stammzertifikat	Das Stammzertifikat befindet sich oben in der Hierarchie in der Zertifikatskette und enthält einen privaten Schlüssel, der zum Signieren anderer Zertifikate verwendet wird. Das Root identifiziert eine bestimmte CA-Organisation. Wenn Sie dieselbe Zertifizierungsstelle für alle Netzwerkgeräte verwenden, benötigen Sie nur ein Stammzertifikat.
Signiertes Zertifikat	Ein Zertifikat, das von einer Zertifizierungsstelle (CA) validiert wird. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Darüber hinaus enthält ein signiertes Zertifikat Details über den Eigentümer des Unternehmens (in der Regel ein Server oder eine Website) und eine digitale Signatur bestehend aus Buchstaben und Zahlen. Ein signiertes Zertifikat nutzt eine Vertrauenskette und wird daher am häufigsten in Produktionsumgebungen verwendet. Auch als „CA-signiertes Zertifikat“ oder als „Managementzertifikat“ bezeichnet.

<b>Laufzeit</b>	<b>Beschreibung</b>
Selbstsigniertes Zertifikat	Ein selbstsigniertes Zertifikat wird vom Eigentümer des Unternehmens validiert. Diese Datendatei enthält einen privaten Schlüssel und stellt sicher, dass Daten verschlüsselt zwischen einem Server und einem Client über eine HTTPS-Verbindung gesendet werden. Es enthält auch eine digitale Signatur, die aus Buchstaben und Zahlen besteht. Ein selbstsigniertes Zertifikat verwendet nicht dieselbe Vertrauenskette wie ein CA-signiertes Zertifikat und wird daher am häufigsten in Testumgebungen eingesetzt. Auch als vorinstalliertes Zertifikat bezeichnet.
Serverzertifikat	Das Server-Zertifikat befindet sich unten in der Zertifikatskette. Es identifiziert Ihre spezifische Einheit, z. B. eine Website oder ein anderes Gerät. Jeder Controller in einem Storage-System benötigt ein separates Serverzertifikat.
Treuhandgeschäft	Ein Truststore ist ein Repository, das Zertifikate von vertrauenswürdigen Drittanbietern, wie z. B. CAS, enthält.
Web Services Proxy	Der Web Services Proxy, der Zugriff über HTTPS-Standardmechanismen bereitstellt, ermöglicht Administratoren die Konfiguration von Managementservices für Speicher-Arrays. Der Proxy kann auf Windows- oder Linux-Hosts installiert werden. Die Unified Manager-Schnittstelle ist im Web Services Proxy enthalten.

## Anleitungen

### CA-signierte Zertifikate verwenden

Sie können CA-signierte Zertifikate für den sicheren Zugriff auf das Verwaltungssystem, das Unified Manager hostet, abrufen und importieren.

#### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

#### Über diese Aufgabe

Die Verwendung von CA-signierten Zertifikaten ist ein zweistufiges Verfahren.

#### Schritt 1: Abschließen und einreichen einer CSR

Sie müssen zuerst eine CSR-Datei (Certificate Signing Request) generieren und sie an die CA senden.

#### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

#### Über diese Aufgabe

Diese Aufgabe beschreibt, wie Sie die CSR-Datei generieren, die Sie an eine CA senden, um signierte, Management-Zertifikate für das System zu erhalten, das Unified Manager hostet, und den Web Services Proxy. Sie müssen Informationen über Ihr Unternehmen sowie die IP-Adresse oder den DNS-Namen des Hostsystems angeben.



Generieren Sie nach der Übermittlung an die CA keine neue CSR. Wenn Sie eine CSR erstellen, erstellt das System ein privates und öffentliches Schlüsselpaar. Der öffentliche Schlüssel ist Teil des CSR, während der private Schlüssel im Schlüsselspeicher aufbewahrt wird. Wenn Sie die signierten Zertifikate erhalten und in den Schlüsselspeicher importieren, stellt das System sicher, dass sowohl der private als auch der öffentliche Schlüssel das ursprüngliche Paar sind. Daher dürfen Sie nach dem Einreichen einer CSR an die CA keine neue CSR generieren. Wenn Sie dies tun, generieren die Controller neue Schlüssel, und die Zertifikate, die Sie von der CA erhalten, funktionieren nicht.

## Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte **Management** die Option **CSR abschließen** aus.
3. Geben Sie die folgenden Informationen ein, und klicken Sie dann auf **Weiter**:
  - **Organisation** — der vollständige, rechtliche Name Ihres Unternehmens oder Ihrer Organisation. Fügen Sie Suffixe wie Inc. Oder Corp. Mit ein
  - **Organisationseinheit (optional)** — die Abteilung Ihrer Organisation, die das Zertifikat bearbeitet.
  - **Stadt/Ort** — die Stadt, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
  - **Bundesland/Region (optional)** — der Staat oder die Region, in der sich Ihr Hostsystem oder Ihr Geschäft befindet.
  - **Land ISO Code** — der zweistellige ISO-Code Ihres Landes (International Organization for Standardization), wie z. B. die USA.
4. Geben Sie die folgenden Informationen über das Host-System ein:
  - **Allgemeiner Name** — die IP-Adresse oder der DNS-Name des Hostsystems, auf dem der Web Services Proxy installiert ist. Stellen Sie sicher, dass diese Adresse korrekt ist, sie muss mit den Angaben übereinstimmen, die Sie für den Zugriff auf Unified Manager im Browser eingeben. Verwenden Sie kein http:// oder https://.
  - **Alternative IP-Adressen** — Wenn der allgemeine Name eine IP-Adresse ist, können Sie optional weitere IP-Adressen oder Aliase für das Host-System eingeben. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format.
  - **Alternative DNS-Namen** — Wenn der gemeinsame Name ein DNS-Name ist, geben Sie weitere DNS-Namen für das Host-System ein. Verwenden Sie für mehrere Einträge ein kommagetrenntes Format. Falls es keine alternativen DNS-Namen gibt, aber Sie im ersten Feld einen DNS-Namen eingegeben haben, kopieren Sie diesen Namen hier.
5. Klicken Sie Auf **Fertig Stellen**.

Eine CSR-Datei wird auf Ihr lokales System heruntergeladen. Der Speicherort des Downloads hängt von Ihrem Browser ab.

6. Senden Sie die CSR-Datei an eine CA und fordern Sie signierte Zertifikate im PEM- oder DER-Format an.

## Nachdem Sie fertig sind

Warten Sie, bis die CA die Zertifikatdateien zurückgibt, und gehen Sie dann zu ["Schritt 2: Import Management Zertifikate"](#).

## Schritt 2: Import Management Zertifikate

Nachdem Sie signierte Zertifikate erhalten haben, importieren Sie die Zertifikatskette für das Hostsystem, auf dem die Unified Manager-Schnittstelle installiert ist.

## Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Sie haben eine Anfrage zur Zertifikatssignierung (.CSR-Datei) erstellt und an die CA gesendet.
- Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
- Die Zertifikatdateien werden auf Ihrem lokalen System installiert.
- Wenn die CA ein verkettetes Zertifikat (z. B. eine .p7b-Datei) lieferte, müssen Sie die verkettete Datei in einzelne Dateien entpacken: Das Stammzertifikat, ein oder mehrere Zwischenzertifikate und das Serverzertifikat. Sie können die Windows verwenden `certmgr` Dienstprogramm zum Auspacken der Dateien (Rechtsklick und wählen Sie **Alle Aufgaben > Export**). Wenn die Exporte abgeschlossen sind, wird für jede Zertifikatdatei in der Kette eine CER-Datei angezeigt.

## Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte \* Management\* die Option **Import**.

Es wird ein Dialogfeld zum Importieren der Zertifikatdateien geöffnet.

3. Klicken Sie auf **Durchsuchen**, um zunächst die Root- und Zwischendateien auszuwählen und dann das Serverzertifikat auszuwählen.

Die Dateinamen werden im Dialogfeld angezeigt.

4. Klicken Sie Auf **Import**.

## Ergebnisse

Die Dateien werden hochgeladen und validiert. Die Zertifikatinformationen werden auf der Seite Zertifikatverwaltung angezeigt.

## Managementzertifikate zurücksetzen

Sie können das Managementzertifikat in den ursprünglichen, werkseitig selbstsignierten Status zurücksetzen.

## Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

## Über diese Aufgabe

Diese Aufgabe löscht das aktuelle Managementzertifikat vom Host-System, auf dem der Web Services Proxy und der SANtricity Unified Manager installiert sind. Nach dem Zurücksetzen des Zertifikats wird das Host-System auf das selbstsignierte Zertifikat zurückgesetzt.

## Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie auf der Registerkarte **Verwaltung** die Option **Zurücksetzen**.

Es wird ein Dialogfeld „Zertifikat für die Verwaltung zurücksetzen bestätigen“ geöffnet.

3. Typ `reset` Klicken Sie im Feld auf **Zurücksetzen**.



Nach der Aktualisierung Ihres Browsers kann der Browser den Zugriff auf die Zielseite blockieren und melden, dass die Website HTTP Strict Transport Security verwendet. Diese Bedingung tritt auf, wenn Sie wieder auf selbstsignierte Zertifikate wechseln. Um die Bedingung zu löschen, die den Zugriff auf das Ziel blockiert, müssen Sie die Browserdaten aus dem Browser löschen.

## Ergebnisse

Das System setzt auf die Verwendung des selbstsignierten Zertifikats des Servers zurück. Das System fordert Benutzer daher auf, das selbstsignierte Zertifikat für ihre Sitzungen manuell anzunehmen.

## Importieren Sie Zertifikate für Arrays

Bei Bedarf können Zertifikate für die Speicher-Arrays importiert werden, sodass sie sich mit dem System authentifizieren können, das SANtricity Unified Manager hostet. Zertifikate können von einer Zertifizierungsstelle (CA) signiert oder selbst signiert werden.

### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.
- Wenn Sie vertrauenswürdige Zertifikate importieren, müssen die Zertifikate für die Speicher-Array-Controller mit SANtricity System Manager importiert werden.

### Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte \* Trusted\* aus.

Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder **Import > Certificates**, um ein CA-Zertifikat zu importieren, oder **Import > Self-signierte Speicher-Array-Zertifikate**, um ein selbstsigniertes Zertifikat zu importieren.

Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das...** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.

4. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

Das Zertifikat wird hochgeladen und validiert.

## Anzeigen von Zertifikaten

Sie können zusammenfassende Informationen für ein Zertifikat anzeigen, das die Organisation, die das Zertifikat verwendet, die Behörde, die das Zertifikat ausgestellt hat, den Gültigkeitszeitraum und die Fingerabdrücke (eindeutige Kennungen) umfasst.

### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden keine Zertifikatfunktionen angezeigt.

### Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:

- **Management** — zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
  - **Trusted** — zeigt Zertifikate an, auf die Unified Manager für Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server, zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Um weitere Informationen zu einem Zertifikat anzuzeigen, wählen Sie seine Zeile aus, wählen Sie die Ellipsen am Zeilenende aus und klicken Sie dann auf **Ansicht** oder **Export**.

## Exportieren von Zertifikaten

Sie können ein Zertifikat exportieren, um die vollständigen Details anzuzeigen.

### Bevor Sie beginnen

Um die exportierte Datei zu öffnen, müssen Sie über eine Zertifikatanzeige-Anwendung verfügen.

### Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie eine der folgenden Registerkarten aus:
  - **Management** — zeigt das Zertifikat für das System, das den Web Services Proxy hostet. Ein Managementzertifikat kann von einer Zertifizierungsstelle (CA) selbst signiert oder genehmigt werden. Die Lösung ermöglicht den sicheren Zugriff auf Unified Manager.
  - **Trusted** — zeigt Zertifikate an, auf die Unified Manager für Speicher-Arrays und andere Remote-Server, z. B. einen LDAP-Server, zugreifen kann. Die Zertifikate können von einer Zertifizierungsstelle (CA) ausgestellt oder selbst signiert werden.
3. Wählen Sie auf der Seite ein Zertifikat aus, und klicken Sie dann am Ende der Zeile auf die Ellipsen.
4. Klicken Sie auf **Exportieren** und speichern Sie dann die Zertifikatdatei.
5. Öffnen Sie die Datei in Ihrer Zertifikatanzeige-Anwendung.

## Vertrauenswürdige Zertifikate löschen

Sie können ein oder mehrere nicht mehr benötigte Zertifikate löschen, z. B. ein abgelaufenes Zertifikat.

### Bevor Sie beginnen

Importieren Sie das neue Zertifikat, bevor Sie das alte löschen.



Beachten Sie, dass das Löschen eines Root- oder Zwischenzertifikats mehrere Speicher-Arrays beeinflussen kann, da diese Arrays dieselben Zertifikatdateien gemeinsam nutzen können.

### Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte \* Trusted\* aus.
3. Wählen Sie ein oder mehrere Zertifikate in der Tabelle aus, und klicken Sie dann auf **Löschen**.



Die Funktion **Löschen** steht für vorinstallierte Zertifikate nicht zur Verfügung.

Das Dialogfeld Vertrauenswürdige Zertifikat bestätigen wird geöffnet.

4. Bestätigen Sie den Löschvorgang, und klicken Sie dann auf **Löschen**.

Das Zertifikat wird aus der Tabelle entfernt.

### Lösen Sie nicht vertrauenswürdige Zertifikate

Nicht vertrauenswürdige Zertifikate treten auf, wenn ein Speicher-Array versucht, eine sichere Verbindung zu SANtricity Unified Manager herzustellen, die Verbindung jedoch nicht als sicher bestätigt. Auf der Zertifikatsseite können Sie nicht vertrauenswürdige Zertifikate auflösen, indem Sie ein selbstsigniertes Zertifikat aus dem Speicher-Array importieren oder ein Zertifikat der Zertifizierungsstelle importieren, das von einem vertrauenswürdigen Dritten ausgestellt wurde.

### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das die Berechtigungen für den Sicherheitsadministrator enthält.
- Wenn Sie ein von einer Zertifizierungsstelle signiertes Zertifikat importieren möchten:
  - Sie haben für jeden Controller im Speicher-Array eine Zertifikatsignierungsanforderung (.CSR-Datei) generiert und an die CA gesendet.
  - Die CA hat vertrauenswürdige Zertifikatdateien zurückgegeben.
  - Die Zertifikatdateien sind auf Ihrem lokalen System verfügbar.

### Über diese Aufgabe

Möglicherweise müssen Sie zusätzliche vertrauenswürdige CA-Zertifikate installieren, wenn eine der folgenden Optionen zutrifft:

- Sie haben kürzlich ein Speicher-Array hinzugefügt.
- Ein oder beide Zertifikate sind abgelaufen.
- Ein oder beide Zertifikate werden widerrufen.
- Ein oder beide Zertifikate fehlen ein Stammzertifikat oder ein Zwischenzertifikat.

### Schritte

1. Wählen Sie **Zertifikatverwaltung**.
2. Wählen Sie die Registerkarte \* Trusted\* aus.

Auf dieser Seite werden alle Zertifikate angezeigt, die für die Speicher-Arrays gemeldet wurden.

3. Wählen Sie entweder **Import > Zertifikate**. So importieren Sie ein CA-Zertifikat oder **Import > Self-signierte Speicher-Array-Zertifikate**, um ein selbstsigniertes Zertifikat zu importieren.

Um die Ansicht einzuschränken, können Sie das Filterfeld **Zertifikate anzeigen verwenden, das...** ist, oder Sie können die Zertifikatzeilen sortieren, indem Sie auf eine der Spaltenüberschrift klicken.

4. Wählen Sie im Dialogfeld das Zertifikat aus und klicken Sie dann auf **Import**.

Das Zertifikat wird hochgeladen und validiert.

# Zugriffsmanagement

## Konzepte

### Funktionsweise von Access Management

Verwenden Sie die Zugriffsverwaltung, um die Benutzerauthentifizierung in SANtricity Unified Manager einzurichten.

#### Konfigurationsworkflow

Die Zugriffsmanagement-Konfiguration funktioniert wie folgt:

1. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren enthält.



Bei der ersten Anmeldung wird der Benutzername verwendet `admin`. Wird automatisch angezeigt und kann nicht geändert werden. Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System. Das Passwort muss bei der ersten Anmeldung festgelegt werden.

2. Der Administrator navigiert zur Zugriffsverwaltung in der Benutzeroberfläche, die vorkonfigurierte lokale Benutzerrollen enthält. Diese Rollen sind eine Implementierung von RBAC-Funktionen (rollenbasierte Zugriffssteuerung).
3. Der Administrator konfiguriert eine oder mehrere der folgenden Authentifizierungsmethoden:
  - **Lokale Benutzerrollen** — Authentifizierung wird über RBAC-Funktionen verwaltet. Lokale Benutzerrollen umfassen vordefinierte Benutzer und Rollen mit bestimmten Zugriffsberechtigungen. Administratoren können diese lokalen Benutzerrollen als einzige Authentifizierungsmethode verwenden oder in Kombination mit einem Verzeichnisdienst verwenden. Es ist keine Konfiguration erforderlich – abgesehen von der Festlegung von Passwörtern für die Benutzer.
  - **Directory Services** — die Authentifizierung wird über einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst verwaltet, z. B. über Microsoft Active Directory. Ein Administrator stellt eine Verbindung zum LDAP-Server her und ordnet die LDAP-Benutzer den lokalen Benutzerrollen zu.
4. Der Administrator stellt Benutzern die Anmeldeinformationen für Unified Manager zur Verfügung.
5. Benutzer melden sich beim System an, indem sie ihre Anmeldedaten eingeben. Während der Anmeldung führt das System die folgenden Hintergrundaufgaben aus:
  - Authentifiziert Benutzernamen und Kennwort anhand des Benutzerkontos.
  - Legt die Berechtigungen des Benutzers basierend auf den zugewiesenen Rollen fest.
  - Bietet dem Benutzer Zugriff auf Funktionen in der Benutzeroberfläche.
  - Zeigt den Benutzernamen im oberen Banner an.

#### Funktionen in Unified Manager verfügbar

Der Zugriff auf Funktionen hängt von den zugewiesenen Rollen eines Benutzers ab. Dazu gehören:

- **Storage Admin** — Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.

- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Eine nicht verfügbare Funktion ist entweder ausgegraut oder wird in der Benutzeroberfläche nicht angezeigt.

## Terminologie für das Zugriffsmanagement

Erfahren Sie, wie die Bedingungen für das Zugriffsmanagement für SANtricity Unified Manager gelten.

Laufzeit	Beschreibung
Active Directory	Active Directory (AD) ist ein Microsoft-Verzeichnisdienst, der LDAP für Windows-Domänennetzwerke verwendet.
Verbindlich	Bindevorgänge werden zur Authentifizierung von Clients auf dem Verzeichnisserver verwendet. Binding erfordert in der Regel Konto- und Kennwortanmeldeinformationen, aber einige Server erlauben anonyme Bindevorgänge.
CA	Eine Zertifizierungsstelle (CA) ist eine vertrauenswürdige Einheit, die elektronische Dokumente, sogenannte digitale Zertifikate, für Internet-Sicherheit ausstellt. Diese Zertifikate identifizieren Website-Besitzer, die sichere Verbindungen zwischen Clients und Servern ermöglichen.
Zertifikat	Ein Zertifikat identifiziert den Eigentümer einer Website aus Sicherheitsgründen, wodurch Angreifer die Identität der Website nicht mehr verkörpern können. Das Zertifikat enthält Informationen über den Websiteeigentümer und die Identität des vertrauenswürdigen Unternehmens, der diese Informationen bescheinigt (unterzeichnet).
LDAP	Lightweight Directory Access Protocol (LDAP) ist ein Anwendungsprotokoll für den Zugriff auf verteilte Verzeichnisdienste und die Wartung. Mit diesem Protokoll können viele verschiedene Anwendungen und Dienste eine Verbindung zum LDAP-Server zur Überprüfung von Benutzern herstellen.
RBAC	Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ist eine Methode zur Regulierung des Zugriffs auf Computer- oder Netzwerkressourcen, basierend auf den Rollen einzelner Benutzer. Unified Manager enthält vordefinierte Rollen.
SSO	Bei Single Sign On (SSO) handelt es sich um einen Authentifizierungsservice, mit dem ein Satz an Anmeldeinformationen auf mehrere Anwendungen zugreifen kann.

Laufzeit	Beschreibung
Web Services Proxy	Der Web Services Proxy, der Zugriff über HTTPS-Standardmechanismen bereitstellt, ermöglicht Administratoren die Konfiguration von Managementservices für Speicher-Arrays. Der Proxy kann auf Windows- oder Linux-Hosts installiert werden. Die Unified Manager-Schnittstelle ist mit dem Web Services Proxy verfügbar.

### Berechtigungen für zugeordnete Rollen

Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen vordefinierte Benutzer, wobei eine oder mehrere Rollen zugewiesen sind. Jede Rolle umfasst Berechtigungen für den Zugriff auf Aufgaben in SANtricity Unified Manager.

Die Rollen ermöglichen Benutzern den Zugriff auf Aufgaben wie folgt:

- **Storage Admin** — Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.

Wenn ein Benutzer über keine Berechtigungen für eine bestimmte Funktion verfügt, ist diese Funktion entweder zur Auswahl nicht verfügbar oder wird nicht in der Benutzeroberfläche angezeigt.

### Zugriffsverwaltung mit lokalen Benutzerrollen

Administratoren können die in SANtricity Unified Manager erzwungenen RBAC-Funktionen (rollenbasierte Zugriffssteuerung) nutzen. Diese Funktionen werden als „lokale Benutzerrollen“ bezeichnet.

#### Konfigurationsworkflow

Lokale Benutzerrollen sind im System vorkonfiguriert. Um lokale Benutzerrollen für die Authentifizierung zu verwenden, können Administratoren Folgendes tun:

1. Ein Administrator meldet sich bei Unified Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren enthält.



Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Ein Administrator überprüft die Benutzerprofile, die vordefiniert sind und nicht geändert werden können.
3. **Optional:** der Administrator weist für jedes Benutzerprofil neue Passwörter zu.
4. Benutzer melden sich mit ihren zugewiesenen Anmeldedaten am System an.

## Vereinfachtes

Bei der Verwendung von nur lokalen Benutzerrollen für die Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

- Passwörter ändern.
- Legen Sie eine Mindestlänge für Passwörter fest.
- Benutzern erlauben, sich ohne Passwörter anzumelden.

## Zugriffsmanagement mit Verzeichnisdiensten

Administratoren können einen LDAP-Server (Lightweight Directory Access Protocol) und einen Verzeichnisdienst wie Microsoft Active Directory verwenden.

### Konfigurationsworkflow

Wenn ein LDAP-Server und ein Verzeichnisdienst im Netzwerk verwendet werden, funktioniert die Konfiguration wie folgt:

1. Ein Administrator meldet sich bei SANtricity Unified Manager mit einem Benutzerprofil an, das die Berechtigungen für Sicherheitsadministratoren enthält.



Der `admin` Benutzer hat vollen Zugriff auf alle Funktionen im System.

2. Der Administrator gibt die Konfigurationseinstellungen für den LDAP-Server ein. Zu den Einstellungen gehören der Domain-Name, die URL und die Bind-Kontoinformationen.
3. Wenn der LDAP-Server ein sicheres Protokoll (LDAPS) verwendet, lädt der Administrator eine Zertifikatskette für die Authentifizierung zwischen dem LDAP-Server und dem Hostsystem, auf dem der Web Services Proxy installiert ist, hoch.
4. Nachdem die Serververbindung hergestellt wurde, ordnet der Administrator die Benutzergruppen den lokalen Benutzerrollen zu. Diese Rollen sind vordefiniert und können nicht geändert werden.
5. Der Administrator testet die Verbindung zwischen dem LDAP-Server und dem Web Services Proxy.
6. Benutzer melden sich mit ihren zugewiesenen LDAP/Directory Services-Anmeldedaten am System an.

## Vereinfachtes

Bei der Verwendung von Verzeichnisdiensten zur Authentifizierung können Administratoren die folgenden Verwaltungsaufgaben ausführen:

- Fügen Sie einen Verzeichnisserver hinzu.
- Bearbeiten der Einstellungen des Verzeichnisseservers.
- Zuordnen von LDAP-Benutzern zu lokalen Benutzerrollen.
- Entfernen Sie einen Verzeichnisserver.
- Passwörter ändern.
- Legen Sie eine Mindestlänge für Passwörter fest.
- Benutzern erlauben, sich ohne Passwörter anzumelden.

# Anleitungen

## Zeigen Sie lokale Benutzerrollen an

Auf der Registerkarte Lokale Benutzerrollen können Sie die Zuordnungen der Benutzer zu den Standardrollen anzeigen. Diese Zuordnungen sind Teil der RBAC (rollenbasierte Zugriffssteuerung), die im Web Services Proxy für SANtricity Unified Manager durchgesetzt wird.

### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

### Über diese Aufgabe

Die Benutzer und Zuordnungen können nicht geändert werden. Es können nur Passwörter geändert werden.

### Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte \* Lokale Benutzerrollen\* aus.

Die Benutzer sind in der Tabelle aufgeführt:

- **Admin** — Super-Administrator, der Zugriff auf alle Funktionen im System hat. Dieser Benutzer enthält alle Rollen.
- **Storage** — der Administrator, der für die gesamte Storage-Bereitstellung verantwortlich ist. Dieser Benutzer umfasst die folgenden Rollen: Storage-Administrator, Support-Administrator und Monitor.
- **Sicherheit** — der für die Sicherheitskonfiguration verantwortliche Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung. Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor.
- **Support** — der Benutzer, der für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die folgenden Rollen: Unterstützen Sie Admin und Monitor.
- **Monitor** — ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieser Benutzer enthält nur die Rolle „Monitor“.
- **rw** (lesen/schreiben) — dieser Benutzer enthält die folgenden Rollen: Speicheradministrator, Supportadministrator und Monitor.
- **Ro** (schreibgeschützt) — dieser Benutzer enthält nur die Rolle Monitor.

## Passwörter ändern

Sie können die Benutzerpasswörter für jeden Benutzer in der Zugriffsverwaltung ändern.

### Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.
- Sie müssen das lokale Administratorkennwort kennen.

### Über diese Aufgabe

Beachten Sie bei der Auswahl eines Passworts die folgenden Richtlinien:



- Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Einstellung für ein Mindestpasswort erfüllen oder überschreiten (unter „Einstellungen anzeigen/bearbeiten“).
- Bei Passwörtern wird die Groß-/Kleinschreibung berücksichtigt.
- Nachgestellte Leerzeichen werden nicht aus Kennwörtern entfernt, wenn sie gesetzt sind. Achten Sie darauf, Leerzeichen einzugeben, wenn diese im Passwort enthalten waren.
- Um die Sicherheit zu erhöhen, verwenden Sie mindestens 15 alphanumerische Zeichen, und ändern Sie das Passwort häufig.

### Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte \* Lokale Benutzerrollen\* aus.
3. Wählen Sie einen Benutzer aus der Tabelle aus.

Die Schaltfläche **Passwort ändern** steht zur Verfügung.

4. Wählen Sie **Passwort Ändern**.

Das Dialogfeld **Passwort ändern** wird geöffnet.

5. Wenn für lokale Benutzerpasswörter keine Mindestkennwortlänge festgelegt ist, können Sie das Kontrollkästchen aktivieren, damit der Benutzer ein Passwort für den Zugriff auf das System eingeben muss.
6. Geben Sie das neue Kennwort für den ausgewählten Benutzer in die beiden Felder ein.
7. Geben Sie Ihr lokales Administratorpasswort ein, um diesen Vorgang zu bestätigen, und klicken Sie dann auf **Ändern**.

### Ergebnisse

Wenn der Benutzer derzeit angemeldet ist, wird die aktive Sitzung des Benutzers durch die Kennwortänderung beendet.

### Ändern Sie die Einstellungen für das lokale Benutzerpasswort

Sie können die erforderliche Mindestlänge für alle neuen oder aktualisierten lokalen Benutzerpasswörter festlegen. Außerdem können lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen.

### Bevor Sie beginnen

- Sie müssen als lokaler Administrator angemeldet sein, der Root-Admin-Berechtigungen enthält.

### Über diese Aufgabe

Beachten Sie die folgenden Richtlinien, wenn Sie die Mindestlänge für lokale Benutzerpasswörter festlegen:

- Die Einstellung von Änderungen hat keine Auswirkung auf vorhandene lokale Benutzerpasswörter.
- Die Mindestlänge für lokale Benutzerpasswörter muss zwischen 0 und 30 Zeichen liegen.
- Alle neuen lokalen Benutzerpasswörter müssen die aktuelle Mindestlängeneinstellung erfüllen oder überschreiten.
- Legen Sie keine Mindestlänge für das Passwort fest, wenn lokale Benutzer ohne Eingabe eines Kennworts auf das System zugreifen möchten.

## Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte \* Lokale Benutzerrollen\* aus.
3. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

Das Dialogfeld **Lokale Benutzerpassworteinstellungen** wird geöffnet.

4. Führen Sie einen der folgenden Schritte aus:
  - Um lokalen Benutzern den Zugriff auf das System zu ermöglichen *ohne* ein Passwort einzugeben, deaktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“.
  - Um eine Mindestkennwortlänge für alle lokalen Benutzerpasswörter festzulegen, aktivieren Sie das Kontrollkästchen „Alle lokalen Benutzerpasswörter müssen mindestens sein“. Verwenden Sie dann das Spinner-Feld, um die erforderliche Mindestlänge für alle lokalen Benutzerpasswörter festzulegen.

Neue lokale Benutzerpasswörter müssen die aktuelle Einstellung erfüllen oder überschreiten.

5. Klicken Sie Auf **Speichern**.

## Verzeichnisserver hinzufügen

Um die Authentifizierung für die Zugriffsverwaltung zu konfigurieren, stellen Sie eine Kommunikation zwischen einem LDAP-Server und dem Host her, auf dem der Web Services Proxy für SANtricity Unified Manager ausgeführt wird. Anschließend ordnen Sie die LDAP-Benutzergruppen den lokalen Benutzerrollen zu.

### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
- LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich Domänenname, Server-URL und optional Benutzername und Kennwort für das Bindekonto.
- Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette des LDAP-Servers auf Ihrem lokalen Computer installiert sein.

### Über diese Aufgabe

Das Hinzufügen eines Verzeichnisseservers ist ein zweistufiger Prozess. Geben Sie zuerst den Domain-Namen und die URL ein. Wenn Ihr Server ein sicheres Protokoll verwendet, müssen Sie auch ein CA-Zertifikat zur Authentifizierung hochladen, wenn es von einer nicht standardmäßigen Signierungsbehörde signiert ist. Wenn Sie über Anmeldedaten für ein Bindekonto verfügen, können Sie auch Ihren Benutzernamen und Ihr Kennwort eingeben. Als Nächstes werden die Benutzergruppen des LDAP-Servers lokalen Benutzerrollen zugeordnet.

## Schritte


1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie auf der Registerkarte **Directory Services** die Option **Add Directory Server** aus.

Das Dialogfeld **Directory Server hinzufügen** wird geöffnet.

3. Geben Sie auf der Registerkarte **Server-Einstellungen** die Anmeldeinformationen für den LDAP-Server ein.

## Felddetails

Einstellung	Beschreibung
<b>Konfigurationseinstellungen</b>	Domäne(en)
Geben Sie den Domänennamen des LDAP-Servers ein. Geben Sie für mehrere Domänen die Domänen in eine kommasetrennte Liste ein. Der Domänenname wird in der Anmeldung ( <i>username@Domain</i> ) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Geben Sie die URL für den Zugriff auf den LDAP-Server in Form von ein <code>ldap[s]://host:port</code> .	Zertifikat hochladen (optional)

Einstellung	Beschreibung
<div data-bbox="245 396 302 453"></div> <p data-bbox="358 170 477 678">Dieses Feld wird nur angezeigt, wenn ein LDAPS-Protokoll im obigen Feld Server-URL angegeben wird.</p> <p data-bbox="212 726 509 1098">Klicken Sie auf <b>Durchsuchen</b> und wählen Sie ein CA-Zertifikat zum Hochladen aus. Dies ist das vertrauenswürdige Zertifikat oder die Zertifikatskette, die für die Authentifizierung des LDAP-Servers verwendet wird.</p>	<p data-bbox="529 159 818 191">Konto binden (optional)</p>
<p data-bbox="212 1150 513 1801">Geben Sie ein schreibgeschütztes Benutzerkonto ein, um Suchanfragen auf dem LDAP-Server und für die Suche in den Gruppen durchzuführen. Geben Sie den Kontonamen im LDAP-Format ein. Wenn der Bindebenutzer beispielsweise „bind-Konto“ heißt, können Sie einen Wert wie eingeben CN=bindacct,CN=Users,DC=cpoc,DC=local.</p>	<p data-bbox="529 1150 834 1182">Bindepaswort (optional)</p>

Einstellung	Beschreibung
<div data-bbox="245 296 302 348"></div> <p data-bbox="362 170 480 443">Dieses Feld wird angezeigt, wenn Sie ein Bindungskonto eingeben.</p> <p data-bbox="215 520 423 615">Geben Sie das Passwort für das Bindekonto ein.</p>	<p data-bbox="529 159 1252 191">Testen Sie die Serververbindung, bevor Sie sie hinzufügen</p>
<p data-bbox="215 674 508 1524">Aktivieren Sie dieses Kontrollkästchen, wenn Sie sicherstellen möchten, dass das System mit der eingegebenen LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt, nachdem Sie unten im Dialogfeld auf <b>Hinzufügen</b> geklickt haben. Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht hinzugefügt. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration hinzuzufügen.</p>	<p data-bbox="529 674 915 705"><b>Berechtigungs-Einstellungen</b></p>
<p data-bbox="215 1577 431 1608">Basis-DN suchen</p>	<p data-bbox="529 1577 1344 1640">Geben Sie den LDAP-Kontext ein, um nach Benutzern zu suchen, normalerweise in Form von CN=Users, DC=copc, DC=local.</p>
<p data-bbox="215 1703 493 1734">Attribut Benutzername</p>	<p data-bbox="529 1703 1414 1766">Geben Sie das Attribut ein, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: sAMAccountName.</p>
<p data-bbox="215 1829 444 1860">Gruppenattribut(e)</p>	<p data-bbox="529 1829 1446 1923">Geben Sie eine Liste der Gruppenattribute für den Benutzer ein, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: memberOf, managedObjects.</p>

4. Klicken Sie auf die Registerkarte **Rollenzuordnung**.
5. Weisen Sie den vordefinierten Rollen LDAP-Gruppen zu. Einer Gruppe können mehrere Rollen zugewiesen sein.

#### Felddetails

Einstellung	Beschreibung
<b>Zuordnungen</b>	Gruppen-DN
Geben Sie den Group Distinguished Name (DN) für die zu zugeordnete LDAP-Benutzergruppe an.	Rollen



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich.

6. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.
7. Wenn Sie mit den Zuordnungen fertig sind, klicken Sie auf **Hinzufügen**.

Das System führt eine Validierung durch und stellt sicher, dass das Speicher-Array und der LDAP-Server kommunizieren können. Wenn eine Fehlermeldung angezeigt wird, überprüfen Sie die im Dialogfeld eingegebenen Anmeldeinformationen, und geben Sie die Informationen ggf. erneut ein.

### Bearbeiten Sie die Einstellungen des Verzeichnisseservers und die Rollenzuordnungen

Wenn Sie zuvor einen Verzeichnisserver in der Zugriffsverwaltung konfiguriert haben, können Sie dessen Einstellungen jederzeit ändern. Zu den Einstellungen gehören die Informationen zur Serververbindung und die Zuordnungen von Gruppen zu Rollen.

#### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.
- Ein Verzeichnisserver muss definiert werden.

#### Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wenn mehr als ein Server definiert ist, wählen Sie den Server aus der Tabelle aus, den Sie bearbeiten möchten.
4. Wählen Sie **Einstellungen Anzeigen/Bearbeiten**.

Das Dialogfeld **Directory Server Settings** wird geöffnet.

5. Ändern Sie auf der Registerkarte **Server-Einstellungen** die gewünschten Einstellungen.

Einstellung	Beschreibung
<b>Konfigurationseinstellungen</b>	Domäne(en)
Der/die Domänenname(n) des/der LDAP-Server(e). Geben Sie für mehrere Domänen die Domänen in eine kommagetrennte Liste ein. Der Domänenname wird in der Anmeldung ( <i>username@Domain</i> ) verwendet, um anzugeben, gegen welchen Verzeichnisserver sich authentifizieren soll.	Server-URL
Die URL für den Zugriff auf den LDAP-Server in Form von <code>ldap[s]://host:port</code> .	Konto binden (optional)
Das schreibgeschützte Benutzerkonto für Suchabfragen am LDAP-Server und für die Suche in den Gruppen.	Bindepasswort (optional)
Das Kennwort für das Bindekonto. (Dieses Feld wird angezeigt, wenn ein Bindekonto eingegeben wird.)	Testen Sie vor dem Speichern die Serververbindung

Einstellung	Beschreibung
Überprüft, ob das System mit der LDAP-Serverkonfiguration kommunizieren kann. Der Test erfolgt nach dem Klicken auf <b>Speichern</b> . Wenn dieses Kontrollkästchen aktiviert ist und der Test fehlschlägt, wird die Konfiguration nicht geändert. Sie müssen den Fehler beheben oder das Kontrollkästchen deaktivieren, um den Test zu überspringen und die Konfiguration erneut zu bearbeiten.	<b>Berechtigungseinstellungen</b>
Basis-DN suchen	Der LDAP-Kontext für die Suche nach Benutzern, in der Regel in Form von CN=Users, DC=copc, DC=local.
Attribut Benutzername	Das Attribut, das zur Authentifizierung an die Benutzer-ID gebunden ist. Beispiel: sAMAccountName.
Gruppenattribut(e)	Eine Liste der Gruppenattribute für den Benutzer, die für die Zuordnung von Gruppen zu Rollen verwendet werden. Beispiel: memberOf, managedObjects.

6. Ändern Sie auf der Registerkarte **Rollenzuordnung** die gewünschte Zuordnung.

Einstellung	Beschreibung
<b>Zuordnungen</b>	Gruppen-DN
Der Domain-Name für die LDAP-Benutzergruppe, die zugeordnet werden soll.	Rollen



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich.

7. Klicken Sie auf **Weitere Zuordnungen hinzufügen**, um weitere Gruppen-zu-Rolle-Zuordnungen einzugeben.

8. Klicken Sie Auf **Speichern**.

## Ergebnisse



Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

## Verzeichnisserver entfernen

Um die Verbindung zwischen einem Verzeichnisserver und dem Web Services Proxy zu unterbrechen, können Sie die Serverinformationen von der Seite Zugriffsverwaltung entfernen. Sie möchten diese Aufgabe möglicherweise ausführen, wenn Sie einen neuen Server konfiguriert haben und den alten dann entfernen möchten.

### Bevor Sie beginnen

- Sie müssen mit einem Benutzerprofil angemeldet sein, das Sicherheitsadministratorberechtigungen enthält. Andernfalls werden die Zugriffsverwaltungsfunktionen nicht angezeigt.

### Über diese Aufgabe

Nach Abschluss dieser Aufgabe werden alle aktiven Benutzersitzungen beendet. Nur Ihre aktuelle Benutzersitzung bleibt erhalten.

### Schritte

1. Wählen Sie **Zugriffsmanagement**.
2. Wählen Sie die Registerkarte **Directory Services** aus.
3. Wählen Sie in der Liste den Verzeichnisserver aus, den Sie löschen möchten.
4. Klicken Sie Auf **Entfernen**.

Das Dialogfeld **Directory Server entfernen** wird geöffnet.

5. Typ `remove` Klicken Sie im Feld auf **Entfernen**.

Die Konfigurationseinstellungen des Verzeichnisseservers, die Berechtigungseinstellungen und Rollenzuordnungen werden entfernt. Benutzer können sich nicht mehr mit Anmeldeinformationen von diesem Server anmelden.

## FAQs

### Warum kann ich mich nicht anmelden?

Wenn beim Versuch, sich bei SANtricity Unified Manager anzumelden, ein Fehler angezeigt wird, überprüfen Sie die möglichen Ursachen.

Login-Fehler bei Unified Manager können aus einem der folgenden Gründe auftreten:

- Sie haben einen falschen Benutzernamen oder ein falsches Passwort eingegeben.
- Sie verfügen über unzureichende Berechtigungen.
- Der Verzeichnisserver (falls konfiguriert) ist möglicherweise nicht verfügbar. Wenn dies der Fall ist, melden Sie sich mit einer lokalen Benutzerrolle an.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, bis Sie sich erneut anmelden können.

Aus einem der folgenden Gründe können Anmeldefehler bei einem Remote-Speicher-Array auftreten:

- Sie haben ein falsches Kennwort eingegeben.
- Sie haben mehrmals versucht, sich erfolglos anzumelden, was den Sperrmodus ausgelöst hat. Warten Sie 10 Minuten, um sich erneut anzumelden.
- Die maximale Anzahl an Client-Verbindungen, die auf dem Controller verwendet werden, wurde erreicht. Suchen Sie nach mehreren Benutzern oder Clients.

### Was muss ich vor dem Hinzufügen eines Verzeichnisseservers wissen?

Bevor Sie einen Verzeichnisserver in Access Management hinzufügen, müssen Sie bestimmte Anforderungen erfüllen.

- Benutzergruppen müssen in Ihrem Verzeichnisdienst definiert sein.
- LDAP-Serveranmeldeinformationen müssen verfügbar sein, einschließlich Domänenname, Server-URL und optional Benutzername und Kennwort für das Bindekonto.
- Bei LDAPS-Servern mit einem sicheren Protokoll muss die Zertifikatskette des LDAP-Servers auf Ihrem lokalen Computer installiert sein.

### Was muss ich über die Zuordnung von Speicher-Array-Rollen wissen?

Überprüfen Sie die Richtlinien, bevor Sie Gruppen zu Rollen zuordnen.

Die RBAC-Funktionen (rollenbasierte Zugriffssteuerung) umfassen folgende Rollen:

- **Storage Admin** — Vollständiger Lese-/Schreibzugriff auf Speicherobjekte auf den Arrays, aber kein Zugriff auf die Sicherheitskonfiguration.
- **Security Admin** — Zugriff auf die Sicherheitskonfiguration in Access Management und Certificate Management.
- **Support Admin** — Zugriff auf alle Hardware-Ressourcen auf Speicher-Arrays, Ausfalldaten und MEL-Ereignisse. Kein Zugriff auf Speicherobjekte oder die Sicherheitskonfiguration.
- **Monitor** — schreibgeschützter Zugriff auf alle Speicherobjekte, aber kein Zugriff auf die Sicherheitskonfiguration.



Die Überwachungsrolle ist für alle Benutzer, einschließlich des Administrators, erforderlich.

Wenn Sie einen LDAP-Server (Lightweight Directory Access Protocol) und Verzeichnisdienste verwenden, stellen Sie sicher, dass:

- Ein Administrator hat im Verzeichnisdienst Benutzergruppen definiert.
- Sie kennen die Gruppen-Domain-Namen für die LDAP-Benutzergruppen.

### Welche lokalen Benutzer gibt es?

Lokale Benutzer sind im System vordefiniert und enthalten bestimmte Berechtigungen.

Zu den lokalen Benutzern gehören:

- **Admin** — Super-Administrator, der Zugriff auf alle Funktionen im System hat. Dieser Benutzer enthält alle Rollen. Das Passwort muss bei der ersten Anmeldung festgelegt werden.
- **Storage** — der Administrator, der für die gesamte Storage-Bereitstellung verantwortlich ist. Dieser

Benutzer umfasst die folgenden Rollen: Storage-Administrator, Support-Administrator und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.

- **Sicherheit** — der für die Sicherheitskonfiguration verantwortliche Benutzer, einschließlich Zugriffsverwaltung und Zertifikatverwaltung. Dieser Benutzer umfasst die folgenden Rollen: Security Admin und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Support** — der Benutzer, der für Hardware-Ressourcen, Ausfalldaten und Firmware-Upgrades verantwortlich ist. Dieser Benutzer enthält die folgenden Rollen: Unterstützen Sie Admin und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Monitor** — ein Benutzer mit schreibgeschütztem Zugriff auf das System. Dieser Benutzer enthält nur die Rolle „Monitor“. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **rw** (lesen/schreiben) — dieser Benutzer enthält die folgenden Rollen: Speicheradministrator, Supportadministrator und Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.
- **Ro** (schreibgeschützt) — dieser Benutzer enthält nur die Rolle Monitor. Dieses Konto wird deaktiviert, bis ein Kennwort festgelegt ist.

## Copyright-Informationen

Copyright © 2024 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 IRGEND EINER 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.