How to guide:

Deploy the Device Registration Task via System Center Configuration Manager

Use Case: Deploy the device trust installer at scale to multiple machines simultaneously.

Device trust is Okta's solution for contextual access management. On Windows, Okta's device trust solution involves deploying a device trust registration task (installer) to your Windows machines. This installer allows you to deploy the Okta certificate to your Windows machines, so Okta sees each machine as trusted.

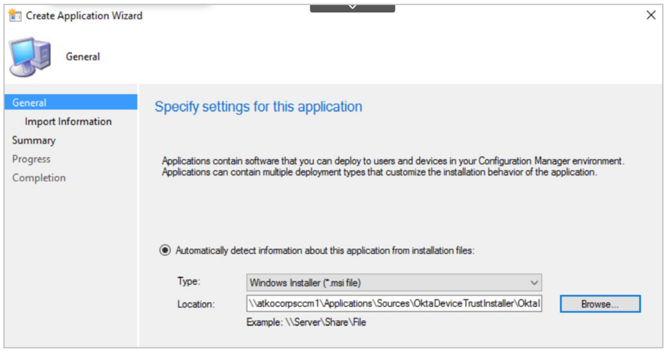
The guide here outlines how you can deploy the device trust registration task via System Center Configuration Manager (SCCM).

Note: *This guide assumes you are using the .msi version of the Device Trust installer, but you can also deploy the .exe with SCCM. The documentation for Okta Device Trust for managed Windows computers is located here.*

Step 1 — Create an application in SCCM with the .msi for the device trust registration task

The first thing that you will want to do is enable the site for pre-release features.

1. In SCCM, head to Software Library—Application Management—Applications. Create a new application. On the General page, choose Automatically detect information about this application from installation files. Browse to the location that the .msi is saved to.



Create Application Wizard

General

Specify settings for this application

Applications contain software that you can deploy to users and devices in your Configuration Manager environment. Applications can contain multiple deployment types that customize the installation behavior of the application.

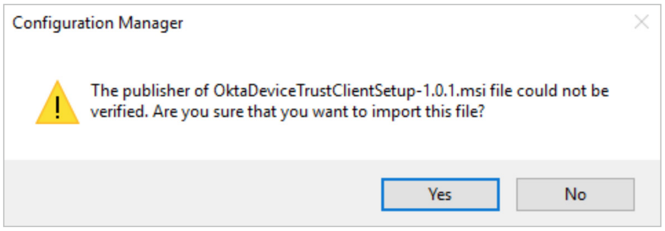
● Automatically detect information about this application from installation files:

Type: Windows Installer (*.msi file)

Location: \\atkocorpsccm1\Applications\Sources\OktaDeviceTrustInstaller\Oktal

Example: \\Server\Share\File

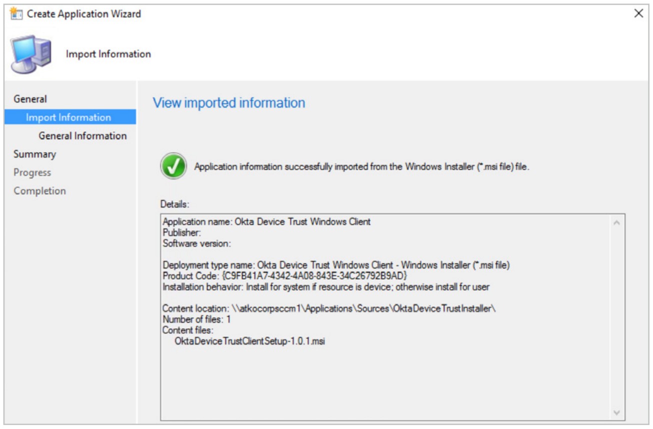
2. You may be prompted with a warning that the Device Trust installer cannot be verified.



Configuration Manager

The publisher of OktaDeviceTrustClientSetup-1.0.1.msi file could not be verified. Are you sure that you want to import this file?

Choose **Yes** here.



View imported information

Application information successfully imported from the Windows Installer (*.msi file) file.

Details:

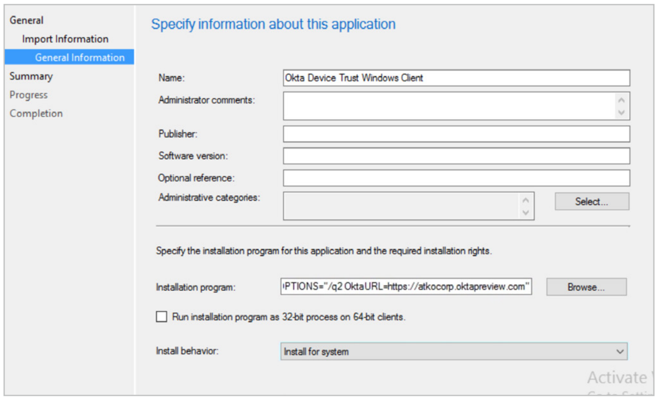
```
Application name: Okta Device Trust Windows Client
Publisher:
Software version:

Deployment type name: Okta Device Trust Windows Client - Windows Installer (*.msi file)
Product Code: {C9FB41A7-4342-4A08-843E-34C26792B9AD}
Installation behavior: Install for system if resource is device; otherwise install for user

Content location: \\atkocorpsccm1\Applications\Sources\OktaDeviceTrustInstaller\
Number of files: 1
Content files:
    OktaDeviceTrustClientSetup-1.0.1.msi
```

3. On the Import Information page, click **Next**.

4. On the **General Information** page, choose a **Name** for this application, and choose any of the other description fields that you require. In the installation program field, choose browse to the location that the .msi is saved, and enter the following command line:

   Note: This command line includes the options for automatic certificate challenge handling. If you do not want to include this as a command line option, refer to the Device Trust for Windows documentation for other command line options.

   msiexec /i OktaDeviceTrustClientSetup-1.x.x.msi INSTALLDIR="c:\Program Files\Okta\DeviceTrust" EXEOPTIONS="/q2 OktaURL=https://<your Okta org>"



Specify information about this application

Name:	Okta Device Trust Windows Client
Administrator comments:	
Publisher:	
Software version:	
Optional reference:	
Administrative categories:	

Specify the installation program for this application and the required installation rights.

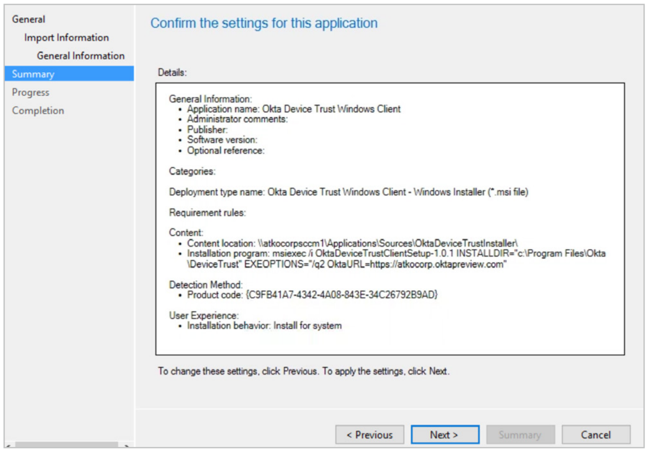
Installation program: ᛁPTIONS="/q2 OktaURL=https://atkocorp.oktapreview.com"

☐ Run installation program as 32-bit process on 64-bit clients.

Install behavior: Install for system

For Install Behavior, choose **Install for system**

5. Click **Next** through the rest of the create application wizard.



Confirm the settings for this application

Details:

General Information:
- Application name: Okta Device Trust Windows Client
- Administrator comments:
- Publisher:
- Software version:
- Optional reference:

Categories:

Deployment type name: Okta Device Trust Windows Client - Windows Installer (*.msi file)

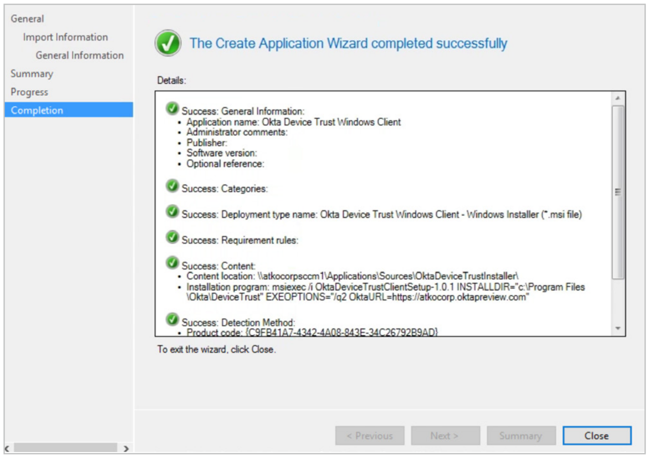
Requirement rules:

Content:
- Content location: \\atkocorpsccm1\Applications\Sources\OktaDeviceTrustInstaller\
- Installation program: msiexec /i OktaDeviceTrustClientSetup-1.0.1 INSTALLDIR="c:\Program Files\Okta\DeviceTrust" EXEOPTIONS="/q2 OktaURL=https://atkocorp.oktapreview.com"

Detection Method:
- Product code: {C9FB41A7-4342-4A08-843E-34C26792B9AD}

User Experience:
- Installation behavior: Install for system

To change these settings, click Previous. To apply the settings, click Next.



The Create Application Wizard completed successfully

Details:

✓ Success: General Information:
- Application name: Okta Device Trust Windows Client
- Administrator comments:
- Publisher:
- Software version:
- Optional reference:

✓ Success: Categories:

✓ Success: Deployment type name: Okta Device Trust Windows Client - Windows Installer (*.msi file)

✓ Success: Requirement rules:

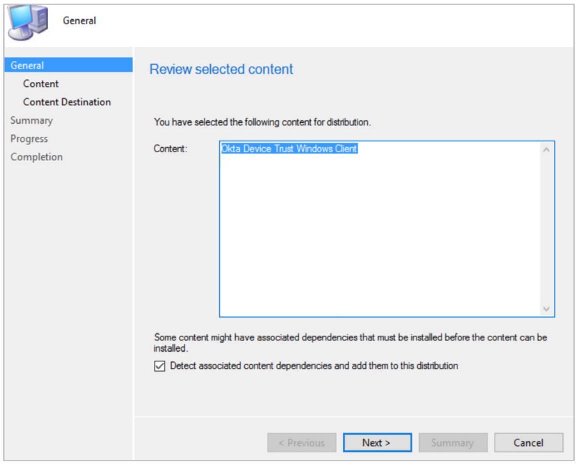
✓ Success: Content:
- Content location: \\atkocorpsccm1\Applications\Sources\OktaDeviceTrustInstaller\
- Installation program: msiexec /i OktaDeviceTrustClientSetup-1.0.1 INSTALLDIR="c:\Program Files\Okta\DeviceTrust" EXEOPTIONS="/q2 OktaURL=https://atkocorp.oktapreview.com"

✓ Success: Detection Method:
- Product code: {C9FB41A7-4342-4A08-843E-34C26792B9AD}

To exit the wizard, click Close.

Step 2 — Distribute the Installer to the Distribution Point

1. Distribute the installer to the Distribution Point. Right click on the application that was just created and choose **Distribute Content.**



Review selected content

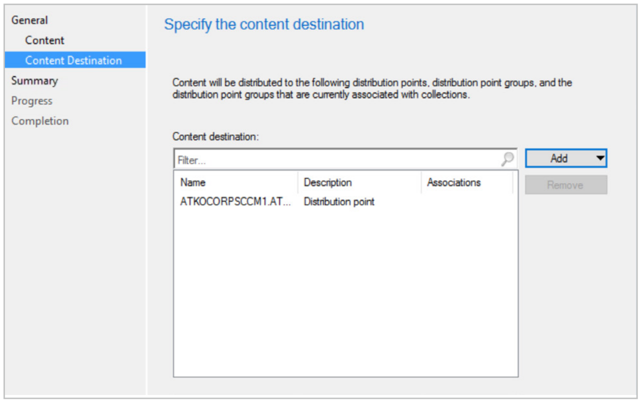
You have selected the following content for distribution.

Content: Okta Device Trust Windows Client

Some content might have associated dependencies that must be installed before the content can be installed.

☑ Detect associated content dependencies and add them to this distribution

2. On the Content Distribution point, choose a Distribution Point.



Specify the content destination

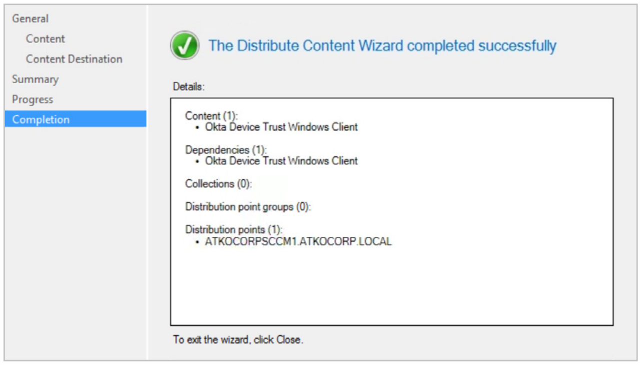
Content will be distributed to the following distribution points, distribution point groups, and the distribution point groups that are currently associated with collections.

Content destination:

Filter...

Name	Description	Associations
ATKOCORPSCCM1.AT...	Distribution point	

3. Click Next through the rest of the Distribute Content Wizard. The application should distribute fairly quickly, and you will see a green Success message in the console.



The Distribute Content Wizard completed successfully

Details:

Content (1):
- Okta Device Trust Windows Client

Dependencies (1):
- Okta Device Trust Windows Client

Collections (0):

Distribution point groups (0):

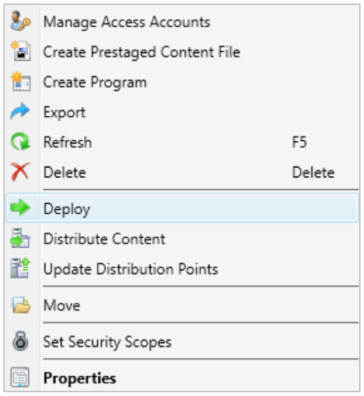
Distribution points (1):
- ATKOCORPSCCM1.ATKOCORP.LOCAL

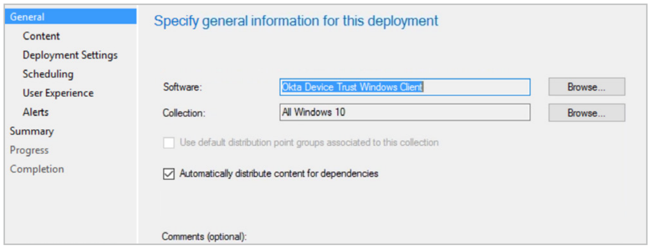
To exit the wizard, click Close.

Step 3 — Deploy the installer to your devices

Once the application has been distributed, it is ready to be deployed to your devices.

1. Right click on the application for the device trust registration task and choose **Deploy**.





Specify general information for this deployment

Software: Okta Device Trust Windows Client

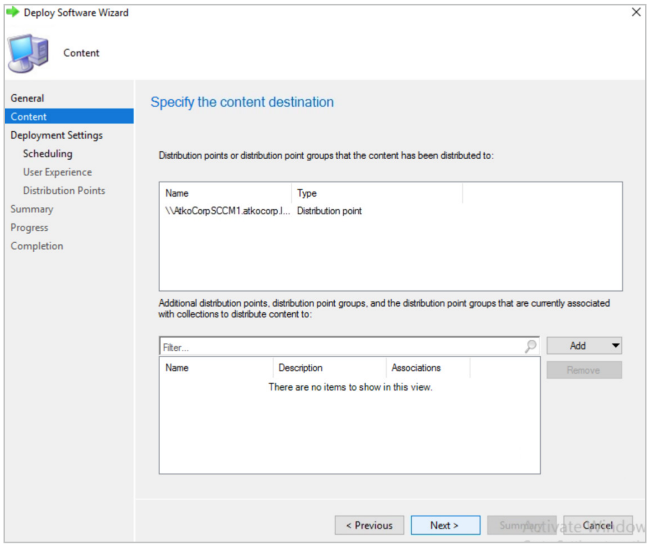
Collection: All Windows 10

□ Use default distribution point groups associated to this collection

☑ Automatically distribute content for dependencies

Comments (optional):

2. Choose a collection to deploy this package to.
3. On the Content page, the Distribution Point that was selected previously should already be listed.
4. Click **Next** through the rest of the deployment. You can choose to deploy as either Required or Available.



Specify the content destination

Distribution points or distribution point groups that the content has been distributed to:

Name	Type
\\AtkoCorpSCCM1.atkocorp.l...	Distribution point

Additional distribution points, distribution point groups, and the distribution point groups that are currently associated with collections to distribute content to:

Filter...

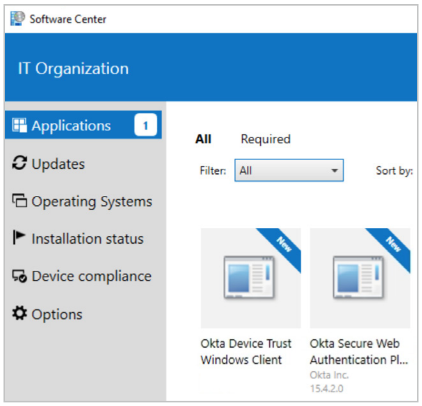
Name	Description	Associations

There are no items to show in this view.

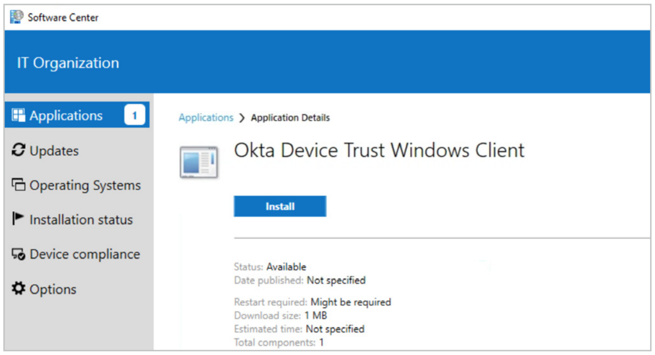
Step 4 — Verify the installation of the Okta device trust registration task

The machine that you validate the install on must be able to connect to the IWA server.

1. You should see that package that you deployed for the Okta CA cert installer listed here.



2. Click **Install**, once the installer runs, the Okta CA certificate will be installed to the Personal user certificate store.

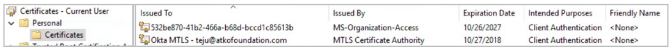


Okta Device Trust Windows Client

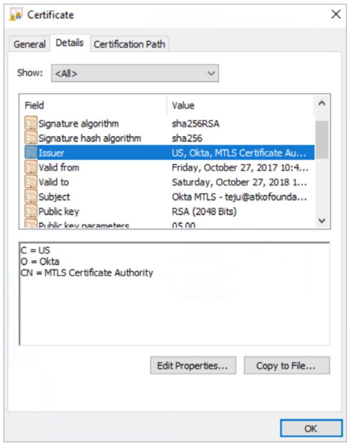
Status: Available
Date published: Not specified
Restart required: Might be required
Download size: 1 MB
Estimated time: Not specified
Total components: 1

3. To verify the install, open certmgr.msc.

4. In the Personal—Certificate store, you will see an Okta MTLS issued certificate.



Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
532be870-41b2-466a-b68d-bccd1c85613b	MS-Organization-Access	10/26/2027	Client Authentication	<None>
Okta MTLS - teju@atkofoundation.com	MTLS Certificate Authority	10/27/2018	Client Authentication	<None>

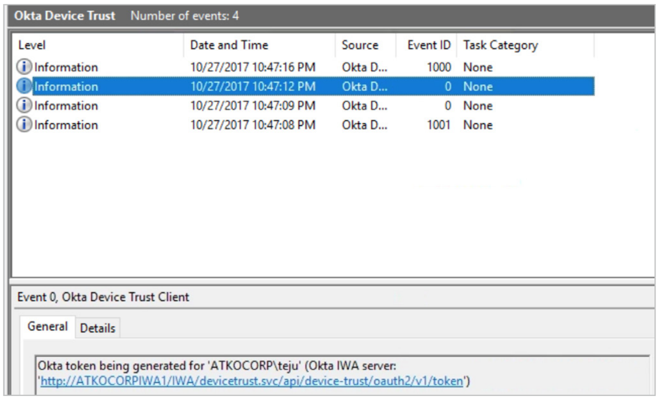


Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	US, Okta, MTLS Certificate Au...
Valid from	Friday, October 27, 2017 10:4...
Valid to	Saturday, October 27, 2018 1...
Subject	Okta MTLS - teju@atkofounda...
Public key	RSA (2048 Bits)
Public key parameters	05 00

C = US
O = Okta
CN = MTLS Certificate Authority

5. Open eventvwr.exe on the same machine, and you will see some entries for the Okta CA certificate issuing process **(Applications and Services Logs—Okta Device Trust).**

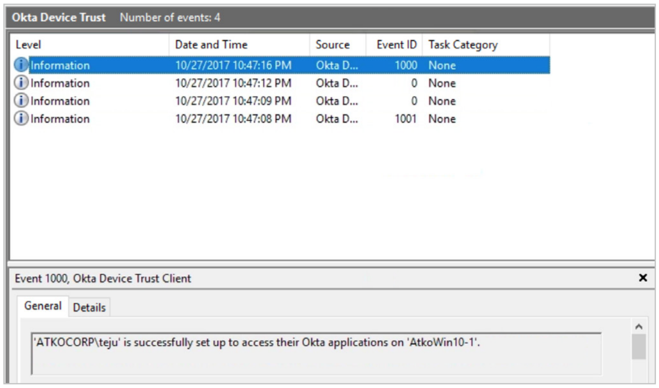


Okta Device Trust Number of events: 4

Level	Date and Time	Source	Event ID	Task Category
Information	10/27/2017 10:47:16 PM	Okta D...	1000	None
Information	10/27/2017 10:47:12 PM	Okta D...	0	None
Information	10/27/2017 10:47:09 PM	Okta D...	0	None
Information	10/27/2017 10:47:08 PM	Okta D...	1001	None

Event 0, Okta Device Trust Client

Okta token being generated for 'ATKOCORP\teju' (Okta IWA server: 'http://ATKOCORPIWA1/IWA/devicetrust.svc/api/device-trust/oauth2/v1/token')



Okta Device Trust Number of events: 4

Level	Date and Time	Source	Event ID	Task Category
Information	10/27/2017 10:47:16 PM	Okta D...	1000	None
Information	10/27/2017 10:47:12 PM	Okta D...	0	None
Information	10/27/2017 10:47:09 PM	Okta D...	0	None
Information	10/27/2017 10:47:08 PM	Okta D...	1001	None

Event 1000, Okta Device Trust Client

'ATKOCORP\teju' is successfully set up to access their Okta applications on 'AtkoWin10-1'.

6. The Okta Device Trust installer is now installed on all Windows machines. You can now use Okta to set up device trust policies for each app via the Okta portal.